Illegal view and copy protection method in digital video system and controlling method thereof

Patent number:	CN1137723
Publication date:	1996-12-11
Inventor:	PARK TAE JOON (KR)
Applicant:	LG ELECTRONICS INC (KR)
Classification:	
- international:	H04N7/167; H04L9/14
- european:	
Application number:	CN19950120389 19951126
Priority number(s):	KR19940031364 19941126

Also published as:

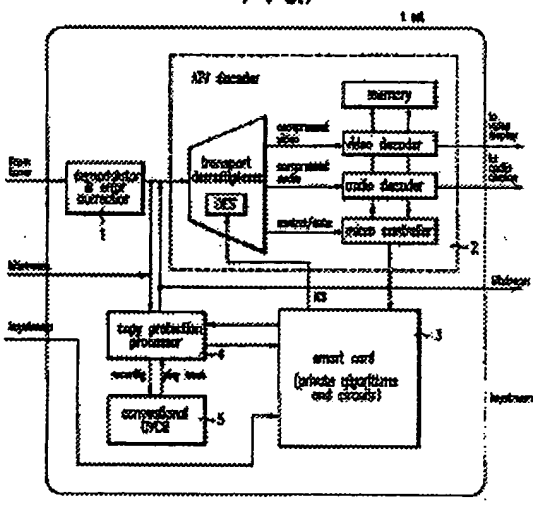
EP0714204 (A2)
US5757909 (A)
JP8242438 (A)
EP0714204 (A3)
EP0714204 (B1)

A front page is attached

Abstract not available for CN1137723
Abstract of corresponding document: **EP0714204**

Illegal view and copy protection method in a digital video system for preventing an illegal user from viewing the digital video system and copying therefrom, by setting a descrambling method which decrypts split keystreams adopting a smart card, including a determination step for determining received data of having been scrambled; a reproduction step, if the received data was determined to be scrambled data in the determination step, splitting the scrambled data into a bitstream and a keystream for decrypting the split keystream for reading in key information, and descrambling the split bitstream according to the read in key information for displaying the bitstream on a display; a recording step for, if the received data was determined to be scrambled data in the determination step, recording the scrambled data on a recording medium either as scrambled data of a bitstream and a keystream according to a recording or copying mode, or after splitting the scrambled data into a bitstream and a keystream, encrypting the split keystream, and mixing the encrypted keystream with the bitstream; and a transporting step, if the received data was determined to be scrambled data in the determination step, splitting the scrambled data into a bitstream and a keystream for transporting the split keystream either after decrypting the split keystream with respect to key information from recording side according to a PPC mode or a back-up copy mode, or after decrypting the split keystream two times with respect to key information of its own and key information from recording side; thereby the reproduction step, the recording step and the transporting step can be performed simultaneously or selectively.

FIG.7



[19]中华人民共和国专利局

[11] 公开号 CN 1137723A

[12] 发明专利申请公开说明书

[21]申请号 95120389.4

[43]公开日 1996 年 12 月 11 日

[51]Int.Cl[6]
H04N 7/167

[22]申请日 95.11.26

[30]优先权

[32]94.11.26[33]KR[31]31364/94

[71]申请人 LG电子株式会社

地址 韩国汉城

[72]发明人 朴兑浚

[74]专利代理机构 柳沈知识产权律师事务所

代理人 黄 敏

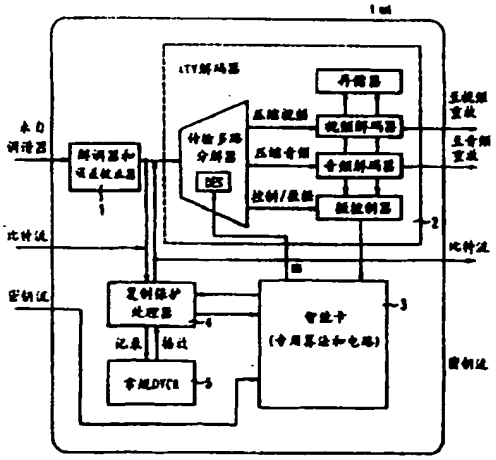
H04L 9/14

权利要求书 10 页 说明书 24 页 附图页数 15 页

[54]发明名称 防止在数字视频系统中非法收看和复制的方法及其控制方法

[57]摘要

防止在数字视频系统中非法收看和复制的方法，通过设定一种采用智能卡解密被分离密钥流的解扰方法防止非法用户收看并复制数字视频系统的节目，包括：确定步骤，用于确定已被扰频的接收数据；重现步骤，将该被扰频数据分离成一个比特流和一个密钥流，记录步骤，对被分离的密钥流加密，并将被加密密钥流与比特流混合；和传输步骤，将扰频数据分离成比特流和密钥流，从而能够同时或有选择地执行重现步骤，记录步骤和传输步骤。



权 利 要 求 书

1、一种防止在数字视频系统中非法收看和复制的方法，包含：

确定步骤，用于确定已被扰频的接收数据；

重现步骤，如果确定所接收的数据是确定步骤中的被扰频数据，将该被扰频数据分离成一个比特流和一个密钥流，用于对用来读入密钥信息的被分离密钥流解密，并根据读入信息对被分离的比特流解扰，以便在显示器上显示比特流；

记录步骤，如果确定所接收的数据是确定步骤中的被扰频数据，或是根据记录或复制方式，作为比特流和密钥流的被扰频数据将该被扰频数据记录在记录介质上，或是在被扰频数据分离成比特流和密钥流之后，对被分离的密钥流加密，并将被加密密钥与比特流混合；和

传输步骤，如果确定所接收的数据是确定步骤中的被扰频数据，将扰频数据分离成比特流和密钥流，或是在根据PPC方式或备份复制方式相对于来自记录一侧的密钥信息对被分离的密钥流解密以后，或是在相对于其本身密钥信息和来自记录一侧的密钥信息对被分离的密钥流解密两次以后传输该被分离密钥流，

从而能够同时或有选择地执行重现步骤，记录步骤和传输步骤。

2、根据权利要求1所述的防止在数字视频系统中非法收看和复制的方法，其中如果确定所接收的数据是确定步骤中的未被扰频数据，则不将所述防止非法收看和复制方法应用到未被扰频的数据。

3、根据权利要求1所述的防止在数字视频系统中非法收看和复

制的方法，其中重现步骤包括用解密算法对所述被分离的密钥解密步骤，用于读入密钥信息。

4、根据权利要求1所述的防止在数字视频系统中非法收看和复制方法，其中记录步骤中的复制操作包括:

第一步骤，用于相对于其本身的密钥信息加密该密钥流，

第二步骤，用于确定被加密的密钥流是备份复制方式或是PPC方式，

第三步骤，如果在第一步骤确定该方式是PPC方式，相对于来自记录一侧的密钥信息对密钥流解密之后，传输的该密钥流加密，然后将被加密的密钥流插入与索引码相对应的位置将其与比特流一起记录，和

第四步骤，如果在第二步骤确定该方式是备份复制方式，对相对于其本身的密钥信息和来自记录一侧的密钥信息对密钥流解密之后所传输的密钥信息相对于来自记录一侧的密钥信息对密钥流加密，并相对于其本身的密钥信息对该被加密密钥流解密，然后将其插入与索引码相对应的位置将其与比特流一起记录。

5、根据权利要求4所述的防止在数字视频系统中非法收看和复制的方法，其中以所述PPC方式操作的第三步骤包括:

第一传输步骤，用于在分离比特流和密钥流之后，传输被扰频的数据并将所述索引码插入所述密钥流的被分离部分，

第二传输步骤，相对于其本身的密钥信息对密钥流加密和相对于来自记录一侧的密钥信息对其解密之后，传输第一传输步骤中分离的密钥流，

记录步骤，相对于来自记录一侧与索引码相一致的密钥信息对

密钥流加密之后，将第二传输步骤中传输的密钥流记录在记录介质上，并将该密钥流与第一传输步骤中传输的比特流混合。

6、根据权利要求5所述的防止在数字视频系统中非法收看和复制的方法，其中记录步骤完成后的重放操作包括：

分离步骤，用于将被重放的比特流分离成一个比特流和一个密钥流，并将索引码插入密钥流的被分离部分，

加密步骤，用于相对于其本身的密钥信息对分离步骤中分离的密钥流加密，

读入步骤，用于相对于其本身的密钥信息通过对加密步骤中被加密的密钥流解密来读入密钥信息，

解密步骤，用于根据读入步骤中读入的密钥信息对被分离的比特流解扰。

7、根据权利要求4所述的防止在数字视频系统中非法收看和复制方法，其中第四步骤中的所述备份复制方式的操作包括：

第一传输步骤，用于在分离被扰频数据为比特流和密钥流之后，传输被扰频的数据并将所述索引码插入所述密钥流的被分离部分，

第二传输步骤，用于在相对于其本身的密钥信息对密钥流加密和相对于来自记录一侧的密钥信息和其本身的密钥信息对被加密的密钥流解密之后，传输第一传输步骤中分离的密钥流。

8、根据权利要求7所述的防止在数字视频系统中非法收看和复制的方法，其中记录步骤完成后的重放操作包括：

分离步骤，用于将被重放的比特流分离成一个比特流和一个密钥流，并将索引码插入密钥流的被分离部分，

加密步骤，用于相对于其本身的密钥信息对分离步骤中分离的

密钥流加密，

读入步骤，用于相对于其本身的密钥信息和MPEG比特流，通过对加密步骤中被加密的密钥流解密两次来读入密钥信息，

解密步骤，用于根据读入步骤中读入的密钥信息对被分离的比特流解扰。

9、一种在数字视频系统中非法收看和复制的方法，包含：

重现步骤，收到被扰频数据时，将该被扰频数据分离成一个比特流和一密钥流，该密钥流用于对用来读入密钥信息的被分离密钥流解密，并根据读入密钥信息对被分离的比特流解扰，以便在显示器上显示比特流；

记录步骤，收到被扰频数据时，将被扰频数据作为比特流和密钥流的被扰频数据记录在记录介质上；

从而能够同时或有选择地执行重现步骤和记录步骤。

10、根据权利要求9所述的防止在数字视频系统中非法收看和复制的方法，其中重放步骤包括通过用于读入密钥信息的解密算法对所述分离的密钥流解密，和通过该读入密钥信息确定解扰方法的步骤。

11、根据权利要求9所述的防止在数字视频系统中非法收看和复制的方法，其中记录步骤完成后的重放操作包括：

分离步骤，用于将被重放的比特流分离成一个比特流和一个密钥流，并将索引码插入密钥流的被分离部分，

加密步骤，用于相对于其本身的密钥信息按照一种加密算法对分离步骤中被分离的密钥流加密，

读入步骤，用于相对于其本身的密钥信息，通过对加密步骤中

被加密的密钥流解密来读入密钥信息，

解密步骤，用于根据读入步骤中读入的密钥信息对被分离的比特流解扰以便在显示屏上显示。

12、一种在复制状态中接收相对于其本身的密钥信息被加密的密钥流的防止在数字视频系统中非法收看和复制的方法，包含：

确定步骤，用于确定是备份复制方式或PPC方式的密钥流方式；

第一传输步骤，如果在确定步骤中确定的方式是PPC方式，相对于来自记录一侧的用于传输密钥流的密钥信息对密钥流解密；

第一记录步骤，相对于来自记录一侧的密钥信息对第一传输步骤中传输的密钥流加密，并将被加密密钥流插入相应于索引码的位置，用于将密钥流和比特流一起记录在记录介质上；

第二传输步骤，如果在确定方式中确定是备份复制方式，相对于其本身的密钥信息和来自记录一侧的用于传输密钥流的密钥信息将密钥流解密两次；和

第二记录步骤，相对于来自记录一侧的密钥信息对第二传输步骤中传输的密钥流加密，并将被加密密钥流插入相当于索引码的位置，用于将密钥流和比特流一起记录在记录介质上。

13、根据权利要求12所述的防止在数字视频系统中非法收看和复制的方法，其中第一传输步骤包括用于对相对于其本身的密钥信息被加密的密钥流相对于其本身的密钥信息解密，和相对于来自记录一侧的其本身的密钥信息对该密钥流再次解密，用于传输该密钥流的步骤。

14、根据权利要求12所述的防止在数字视频系统中非法收看和复制的方法，其中第二传输步骤包括用于对相对于其本身的密钥信

息被解密的比特流相对于其本身的密钥信息解密两次，和相对于来自记录一侧的密钥信息对该密钥流再次解密，用于传输该密钥流的步骤。

15、一种防止在数字视频系统中非法收看和复制的方法，包含：

'PPC' 方式重现步骤，通过检测从记录介质重现的密钥流，已经确定记录介质是'PPC'记录介质时，相对于其本身的密钥信息对密钥流加密，并相对于其本身的用于读入密钥信息的密钥信息对密钥流解密，用于对用来读入密钥信息和索引码这两者的比特流解扰；

'备份复制'方式重现步骤，通过检测从记录介质重现的根据其本身的密钥信息被解密的密钥流，已经确定记录介质是'备份复制'记录介质时，相对于其本身的密钥信息和来自记录一侧的密钥信息将密钥流加密两次并相对于其本身的用于读入密钥信息的密钥信息对密钥流解密，用于对用来写入密钥信息和索引码这两者的比特流解扰。

16、一种防止在数字视频系统中非法收看和复制的设备，包含：

解调&误差校正装置，用于解调广播信号并对所述信号进行RS-解码；

复制保护处理装置，用于将所述解调& 误差校正装置的输出传输到数字记录/重现设备，将从所述数字记录/重现设备重现的被扰频记录信号分离成比特流和密钥流，对被分离的密钥流加密；

解码装置，用于根据解扰信息对来自所述解调& 误差校正装置或复制保护处理装置的比特流解扰；和

一个智能卡，用于对所述复制保护处理装置的被加密密钥流解

密，加到所述解码装置作为解扰信息。

17、根据权利要求16所述的防止在数字视频系统中非法收看和复制的设备，其中所述防止非法收看功能是这样进行的：使连接到所述解调& 误差校正装置的解码装置被连接到所输智能卡，对所述解码装置的密钥流解码，并将解扰信息输出到所述解码装置。

18、根据权利要求16所述的防止在数字视频系统中非法收看和复制的设备，其中第一记录是通过将连到所述解调& 误差校正装置的所述复制保护处理装置连接到所述数字记录/重放设备进行的。

19、根据权利要求16所述的防止在数字视频系统中非法收看和复制的设备，其中防止非法重放是这样进行的：连到所述数字记录/重放设备的所述复制保护处理装置的密钥流线路连接到所述智能卡，比特流线路连接到所述解码装置，所述复制保护处理装置和所述解码装置互相连接，以使所述智能卡将所述复制保护处理装置的密钥流解密成其本身的与所述解码装置的索引码相对应的密钥信息，然后将该密钥流输出到所述解码装置。

20、根据权利要求19所述的防止在数字视频系统中非法收看和复制的设备， 其中以PPC模式从记录介质重放期间，所述保护处理装置相对于其本身的密钥信息对从所述数字记录/重放设备重放的数据分离的密钥流加密两次，并将该密钥流传输到所述智能卡。

21、根据权利要求19所述的防止在数字视频系统中非法收看和复制的设备，其中以备份复制模式从记录介质重放期间，所述保护处理装置相对于其本身的密钥信息对从所述数字记录/重放设备播放的数据分离的密钥流进行多于两次的加密，并将该密钥流传输到所述智能卡。

22、根据权利要求16、18或19之一所述的防止在数字视频系统中非法收看和复制的设备，其中所述复制保护处理装置包括：

一个RAM，用于存储智能卡的固有密钥信息，

一个算法存储存储器，用于存储一种加密算法，和

一个处理器，用于通过所述RAM密钥信息执行所述算法存储存储器的加密程序。

23、根据权利要求16、17或19之一所述的防止在数字视频系统中非法收看和复制的设备，其中所述智能卡包括：

一个第一算法存储存储器，用于存储用于比特流的解密算法程序，

一个第二算法存储存储器，用于存储其本身的解密算法程序，

一个ROM，用于存储其本身的密钥信息，和

一个RAM，用于临时存储另一智能卡的密钥信息。

24、一种防止在数字视频系统中非法收看和复制的设备，包含：

第一复制保护处理装置，用于将来自第一数字记录/重现设备的重现数据分离成比特流和密钥流，并对被分离的密钥流加密；

第一和第二智能卡，相对于其本身的密钥信息和来自记录一侧的密钥信息对来自所述第一复制保护处理装置的被加密密钥流解密；和

第二复制保护处理装置，用于相对于其本身的密钥信息对通过第二智能卡传输到第一智能卡的密钥流加密并将被加密的密钥流和被分离的比特流一起传输到第二数字记录/重现设备，在记录介质上进行记录。

25、根据权利要求24所述的防止在数字视频系统中非法收看和

复制的设备，其中所述第一复制保护处理装置相对于其本身的密钥信息对密钥流加密，并将该密钥流传输到所述第一智能卡。

26、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中所述智能卡相对于其本身的密钥信息和记录一侧的密钥信息对所述第一复制保护处理装置的密钥流解密，并将该密钥流传输到所述第二智能卡。

27、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中所述第二复制保护处理装置相对于其本身的密钥信息对从所述第二智卡传输的密钥流加密，并将该密钥流与来自所述第一复制保护处理装置的比特流混合。

28、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中在备份复制保护模式期间，所述第一智能卡相对于其本身的密钥信息对来自所述第一复制保护处理装置的密钥流解密两次，并相对于来自记录一侧的密钥信息对该密钥流解密。

29、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中所述第二复制保护处理装置相对于其本身的密钥信息对从所述第二智能卡传输的密钥流加密，并将被加密的密钥流与比特流混合。

30、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中所述第一和第二复制保护处理装置的每一个包括：

一个RAM，用于存储所述智能卡的固有密钥信息，

一个算法存储存储器，用于存储一种加密算法，和

一个处理器，用于通过所述RAM密钥信息执行所述算法存储存储器的加密程序。

31、根据权利要求24所述的防止在数字视频系统中非法收看和复制的设备，其中所述第一和第二智能卡的每一个包括:

一个第一算法存储存储器，用于存储用于比特流的解密算法程序，

一个第二算法存储存储器，用于存储其本身的解密算法程序，

一个ROM，用于存储其本身的密钥信息，和

一个RAM，用于临时存储另一个智能卡的密钥信息。

说 明 书

防止在数字视频系统中非法收看和复制的方法及其控制方法

本发明涉及防止在数字视频系统中非法收看和复制的技术，特别是通过设置对使用“智能卡”(smart cart)的分离密钥流进行解密的解扰方法，防止在数字视频系统中非法收看和复制的方法，以阻止非法用户收看数字视频系统并对其进行复制。

在一般的数字视频系统中，实现有条件接入(CA)系统以此来防止非法收看的做法很被人们感兴趣。

在这样一种CA系统中，广播信号在电缆电视或广播的卫星广播服务这类收费信息中被扰频。因此，只有正常附费的用户才能通过适当解扰方法收看节目。

例如，卫星广播接收机或作为美国行进电视(ATV)标准的大联盟(Grand Alliance)(GA)系统具有支持CA的功能。另外，例如由GI制造的能用于卫星广播的视频密码器这类扰频/解扰装置已经被普遍使用。

GI制造的视频密码器一般被用于CA系统的扰频系统，该系统以Gihousen的美国专利No.4,613,901中公开的系统和方法为基础，其中经一个正常用户解扰器传送的电视信号在广播的收费广播TV系统中被扰频，然后在用户解扰器被有选择地解扰。用于执行解扰的视频密码器系统是通过采用美国专利No.5,111,504公开的智能卡实现

的。这样实施使Gihousen提出的系统分为两部分，即，一个与解扰器对应的信息处理器，和一个可以由智能卡替代的保密元件。

因此，通过采用以上方法，扰频系统的实施如图1所示，解扰系统的实施如图2所示。

换句话说，常规的用于防止数字视频系统中违法收看的装置包括一个扰频器101，用于根据普通类型密钥(CK)和一个初始化向量(PK)对TV信号扰频和输出被扰频的TV信号(SVo)，并对信息$E_{U(D)}E_{U(S)}$(CK)和E_{CK}(PK)扰频，一个智能卡103，用于相对于解扰信息U(S)对解扰A(D)和A(S)的信息加密，和一个信息处理器102，用于对解扰$E_{A(D)}[E_{AS}(WK)]$的信息解密，以解扰从扰频器101传送的TV信号(SVo)并将同一信号恢复成原始TV信号DVo。

在这里，A(D)是信息处理器102的鉴别密钥，A(S)是智能卡103的鉴别密钥，U(D)是信息处理器102的一个单元密钥，U(S)是智能卡103的一个单元密钥。

当时，扰频器101包括一个第一加密器111，用于相对于解扰信息U(D)和U(S)对普通类型密钥(CK)加密，和一个第二加密器112，用于相对于普通类型密钥(CK)对初始化向量(PK)加密，一个第三加密器113，用于相对于第二加密器112输出的E_{CK}(PK)对初始化向量(PK)加密和一个扰频执行方114，用于相对于第三加密器113的输出WK对TV信号Vi扰频 。

现在将描述具有上述配置的常规装置的操作。

首先，在传输系统中传输一TV信号的情况下，扰频器101操作，使第一加密器111相对于解扰信息U(D)和U(S)对普通类型密钥(CK)加密，第二加密器112相对于普通类型密钥(CK)对初始化向量(PK)

加密，第三加密器113相对于第二加密器112的输出对E_{CK}(PK)的初始化向量(PK)加密，然后将其输出到扰频执行方114。

当时，扰频执行方114相对于第三加密器113的输出WK对TV信号扰频。在这里扰频信息WK以E_{BCK}(PK)表示。

于是，扰频器101向信息处理器102传送相对于普通类型密钥(CK)加密的信息$E_{U(D)}E_{U(S)}$(CK)，被加密的初始化向量(PK)信息E_{CK}(PK)和被扰频的TV信号SVo。

在对被扰频TV信号解扰的情况下，智能卡103相对于信息处理器102的鉴别信息A(D)和其本身的鉴别信息A(S)对解扰所需的信息WK加密，然后向信息处理器102产生被加密的解扰信息$E_{A(D)}[E_{A(S)}(WK)]$。

于是，信息处理器102对智能卡103产生的被加密解扰信息$E_{A(D)}[E_{A(S)}(WK)]$解密并对用被加密的解扰信息$E_{A(D)}[E_{A(S)}(WK)]$从扰频器101传送的TV信号SVo解扰。从而将其恢复成原始TV信号DVo。

在这里，通过在信息处理器102和智能卡103之间传送信息时采用加密方法来增强防止非法收看和复制的可靠性。

例如，GA-HDTV系统的规格支持CA系统并包括传输协议所需的各种功能。

这些功能的灵活性和实用性在于它们支持所有可能的解扰方法和密钥加密方法，并且比特流被有选择地扰频以使CA功能在用基元流的单元中采用。

在这里，该扰频操作根据信息数据使数据比特流随机化，并且用加密操作转换了信息数据，以防止来自非法用户的信息数据。

换句话说，CA系统使被传送的数据随机化并借助一个扰频器使非法用户的解码器错误解码而无效，但通过提供用于初始化解扰器

电路的信息允许合法用户的解码器正确地对接收的TV广播信号解码。

以这种操作传送MPEG协议的CA由图3所示的格式实现并支持如下的CA功能。

第一， 一个2比特的传输扰频控制字段通知一个传输流是否被扰频和使用哪种扰频密钥。

第二，将每个数据插入使用一个传输专用数据字段的GA传输系统中，该传输专用数据字段位于传输流的适配标题中，被加密的扰频信息存储在该字段。

该CA传输MPEG协议单独或同时地传输一个传输标题、一个分组化的基元流(PES)以及音频和视频数据。 该传输协议包括一个标题的链路标题区、一个适配标题区和一个有效负载区。

在这里，链路标题长度为4字节，适配标题的长度可变。

将传输扰频控制字段插入链路标题。字段值为“00”表示未被扰频，“10”表示偶数密钥，“11”表示奇数密钥，“01”表示被预定。

适配标题包括一个标记符比特和传输专用数据字段，该标记符比特包括1比特的传输专用数据标记符。图3所示的CA传输MPEG协议的PES标题的构成如图4所示。

PES标题中有一个用于数字存储介质(DSM)，例如一个数字盒式录像机(DVCR)的字段。 该字段包括长度为14比特的PES标题标记符区和长度可变的PES标题字段。 PES标题标记符区包括一个1比特的版权(CR)标记符、一个1比特的原版或复制标记符、一个2比特的PD标记符、一个1比特的TM标记符和一个1比特的AC标记符。

PES标题字段具有可变长度并且其区域部分地由包含在PES标题

标记符区中的PD、TM和AC标记符设定。

换句话说，如果PD标记符的值为“00”，PES标题字段中不存在PTS/DTS区，如果PD标记符的值为“10”，存在40比特的PTS/DTS，如果PD标记符的值为“11”，存在80比特的PTS/DTS。如果TM标记符的值为“0”，则不存在DSM策略(trick)方式，如果TM标记符的值为“1”，DSM策略方式则变为8比特。另外，如果设定AC标记符为“1”，一个附加复制信息字段变为8比特。

采用上述格式传输扰频信息，以及使用该信息的解扰过程如图5所示。

在这里，由于解扰系统将下一个被加密密钥与用于当前解扰的密钥一起解密，解扰器至少存储两个密钥，即一个奇数密钥和一个偶数密钥。

另外，扰频系统根据当前传输流的解扰方法设定链路标题中传输扰频控制字段的值，然后将其传输。

因此，解扰器根据来自接收的数据被解密的传输标题的传输扰频控制字段的值确定一个偶数密钥或一个奇数密钥。

换句话说，当传输具有图5所示格式的数据以及解扰器根据在智能卡中被解密的传输扰频控制字段的值解扰第K_{2n-1}帧时，智能卡对下一个被解扰的第K_{2n}帧的传输扰频控制字段解密。这些操作是连续地进行的。

可以按图6所示来实现执行CA功能的ATV解码器。ATV解码器110将一个需要快速操作的解扰器装入传输多路分解器105中并通过DES算法或使用PN序列的流密码算法进行解扰。由ATV解码器110加密的密钥在智能卡103中被解密。这里，智能卡103和ATV解码器110之间

的接口是按ISO-7816标准规定执行。

换句话说，在图6所示的实施例中，从一个调谐器接收的信号在一个解调器&误差校正器104中被解调，然后通过RS解码校正传输期间产生的误差并输入到ATV解码器110的传输多路分解器105，然后被解扰。

当时，一个微控制器109操作被解扰的控制信号和数据并将用于解扰的加密信息传输到智能卡103。智能卡103对传输来的加密信息解密并将其传输到ATV解码器110。

当时，传输多路分解器105根据解扰信息恢复被压缩的视频和音频信号，控制信号和数据。

于是，视频解码器107扩展被压缩的视频信号并将被扩展信号暂时存储在存储器106中，然后输出存储数据显示视频。音频解码器108扩展被压缩的音频信号，然后重放声音。

另外，微控制器109读取从传输多路分解器105输出的控制信号和数据并控制视频解码器107和音频解码器108的操作。

在用于加密的各种方法中，广泛使用块密码算法，例如DES，和使用PN序列的流密码算法。

然而，由于这些方法仅用被加密信号进行加密和解密，很难达到密钥管理和密钥分配。

因此，为解决上述问题，美国专利No.4,200,770提出了公用密钥加密方法。该方法用一个公用密钥进行加密，并用其各自的保密密钥进行解密。

该公用密钥加密方法已经在美国专利No.4,405,829公开的称为RSA的加密算法中被改进，并作为加密系统实施。然而，该公用密

钥加密方法不适用于快速加密。

CA系统的目的在于防止非法收看。 然而，并不能防止通过DSA(例如DVCR)扩散的节目被非法复制。

换句话说， 防止通过记录媒介(例如DSM)扩散节目意味着防止非法复制。 但是，常规的模拟VCR系统中采用的防止复制方法很难用于数字存储媒质。 另外，对用于DSM的防止复制方法的研究仍未发展完善。

为解决现有技术的上述问题，本发明的一个目的是提供防止在数字视频系统中非法收看和复制的方法和用于防止非法收看和复制的控制方法，其中，通过传输一个扰频比特流和用于扰频到不同路径的加密密钥在一个智能卡中将加密密钥解密，并根据该信息将比特流解扰，正常的解码不仅仅通过比特流进行。

本发明的另一个目的是在CA系统中采用智能卡，以便自动进行收费， 以实现收看前附费(PPV)的功能并通过更换智能卡加进各种功能使系统性能升级。

本发明的再一个目的是通过分离传输数据大大降低被保护数据的密钥数量， 并通过通电或连接到数字记录/重现设备进行记录期间鉴别和密钥的自动性能使非法智能卡对该系统无效。

根据本发明的一个方面，提供防止在数字视频系统中非法收看和复制的方法，包括：确定步骤，用于确定已被扰频的接收数据；重现步骤，如果确定所接收的数据是确定步骤中的被扰频数据，将该被扰频数据分离成一个比特流和一个密钥流，用于对用来读入密钥信息的被分离密钥流解密，并根据读入密钥信息对被分离的比特流解扰，以便在显示器上显示比特流；记录步骤，如果确定所接收

的数据是确定步骤中的被扰频数据，或是根据记录或复制方式，作为比特流和密钥流的被扰频数据将该被扰频数据记录在记录介质上，或是在被扰频数据分离成比特流和密钥流之后，对被分离的密钥流加密，并将被加密密钥与比特流混合；和传输步骤，如果确定所接收的数据是确定步骤中的被扰频数据，将扰频数据分离成比特流和密钥流，或是在根据PPC方式或备份复制方式相对于来自记录一侧的密钥信息对被分离的密钥流解密以后，或是在相对于其本身密钥信息和来自记录一侧的密钥信息对被分离的密钥流解密两次以后传输该被分离密钥流，从而能够同时或有选择地执行重现步骤，记录步骤和传输步骤。

根据本发明的另一个方面，提供防止在数字视频系统中非法收看和复制的方法，包括：重现步骤，收到被扰频数据时，将该被扰频数据分离成一个比特流和一个密钥流，用于对用来读入密钥信息的被分离密钥流解密，并根据读入密钥信息对被分离的比特流解扰，以便在显示器上显示比特流；记录步骤，收到被扰频数据时，将被扰频数据作为比特流和密钥流的被扰频数据记录在记录介质上；从而能够同时或有选择地执行重现步骤和记录步骤。

根据本发明的再一个方面，提供防止在数字视频系统中非法收看和复制的方法，包括：确定步骤，用于确定是备份复制方式或PPC方式的密钥流方式；第一传输步骤，如果在确定方式是确定步骤中的PPC方式，相对于来自记录一侧的用于传输密钥流的密钥信息使密钥流解密；第一记录步骤，相对于来自记录一侧的密钥信息对第一传输步骤中传输的密钥流加密，并将被加密密钥流插入相当于索引码的位置，用于将密钥流和比特流一起记录在记录介质上；

第二传输步骤，如果在确定步骤中确定是备份复制方式，相对于其本身的密钥信息和来自记录一侧的用于传输密钥流的密钥信息将密钥流解密两次；和第二记录步骤，相对于来自记录一侧的密钥信息对第二传输步骤中传输的密钥流加密，并将被加密密钥流插入相当于索引码的位置，用于将密钥流和比特流一起记录在记录介质上；

根据本发明的再一个方面，提供防止在数字视频系统中非法收看和复制的方法，包括：‘PPC’方式重现步骤，通过检测从记录介质重现的密钥流，已经确定记录介质是‘PPC’记录介质时，相对于其本身的密钥信息对密钥流加密，并相对于其本身的用于读入密钥信息的密钥信息对密钥流解密，用于对用来读入密钥信息和索引码这两者的比特流解扰；以及‘备份复制’方式记录步骤，通过检测从记录介质重现的相对于其本身的密钥信息被解密的密钥流，已经确定记录介质是‘备份复制’记录介质时，相对于其本身的密钥信息和来自记录一侧的密钥信息将密钥流加密两次并相对于其本身的用于读入密钥信息的密钥信息对密钥流解密，用于对用来写入密钥信息和索引码这两者的比特流解扰。

根据本发明的另一个目的，提供防止在数字视频系统中非法收看和复制的设备，包括：解调&误差校正装置，用于调制/解调模拟广播信号并对所述信号进行RS-解码；复制保护处理装置，用于将所述解调&误差校正装置的输出传输到数字记录/重现设备，将从所述数字记录/重现设备重现的被扰频记录信号分离成比特流和密钥流，对被分离的密钥流加密；解码装置，用于根据解扰信息对来自所述解调&误差校正装置或复制保护处理装置的比特流解扰；和一个智能卡，用于对所述复制保护处理装置的被加密密钥流解密，加

到所述解码装置作为解扰信息。

根据本发明的再一个目的，提供防止在数字视频系统中非法收看和复制的设备，包括：第一复制保护处理装置，用于将来自第一数字记录/重现设备的重现数据分离成比特流和密钥流，并对被分离的密钥流加密；第一和第二智能卡，相对于其本身的密钥信息和来自记录一侧的密钥信息对来自所述第一复制保护处理装置的被加密密钥流解密；和第二复制保护处理装置，用于相对于其本身的密钥信息对通过第二智能卡传输到第一智能卡的密钥流加密并将被加密的密钥流和被分离的比特流一起传输到第二数字记录/重现设备，在记录介质进行记录。

在本发明中，复制保护处理装置包括一个RAM，用于存储智能卡的固有密钥信息，一个算法存储存储器，用于存储一种加密算法，和一个处理器，用于通过RAM密钥信息执行算法存储存储器的加密程序。

上述复制保护处理装置包括CA功能以及包括防止非法收看和防止非法复制的所有节目版权保护功能。

在本发明中，智能卡包括一个第一算法存储存储器，用于存储用于比特流的解密算法程序，一个第二算法存储存储器，用于存储其本身密钥信息的解密算法程序，一个ROM，用于存储其本身的密钥信息，和一个RAM，用于临时存储另一个智能卡的密钥信息。

通过参照附图对优选实施例进行的详细描述，将使本发明的上述目的和优点将变得显而易见，其中：

图1是普通扰频器的方框图；

图2是普通解扰器的方框图；

图3示出传输格式；

图4详细示出图3所示PES标题；

图5通过密钥分布示出传输格式；

图6是常规ATV解码器的方框图；

图7是根据本发明的防止非法收看和复制装置的方框图；

图8是图7所示复制保护装置的详细方框图；

图9是图7所示智能卡的详细方框图；

图10示出图8所示比特流的分离；

图11示出各个比特流的格式；

图12至图18示出本发明的连接方式；

图19和图20示出操作本发明的信号流程；和

图21示出根据本发明的密钥交换和鉴别的信号流程。

本发明适用于所有能记录和重现数字信号的记录/重现设备，为便于说明，下文描述的是在DVCR情况下的实施例，在这里作为例子。

因此，如图7所示，根据本发明实施例的防止数字视系统中非法收看和复制的设备，包括一个解调&误差校正器1，用于调制/解调模拟广播信号并对所述信号进行RS-解码，一个ATV解码器2，用于根据解扰信息对解调&误差校正器1的输出进行解扰，一个复制保护处理器4，用于将被扰频的记录信号分离成比特流和密钥流并对被分离的密钥流加密；和一个智能卡3，用于对所述复制保护处理器4的被分离和加密的密钥流以及ATV解码器2的索引码进行解密，并将解扰信息KS输出到ATV解码器2。

如图8所示，复制保护处理器4包括一个RAM 17，用于存储智能

卡的固有密钥信息，一个算法存储存储器18，用于存储一种加密算法，和一个处理器19，用于执行算法存储存储器的加密程序通过RAM 17的密钥信息。

如图9所示，智能卡3包括一个第一算法存储存储器12，用于存储用于比特流的解密算法程序，一个第二算法存储存储器13，用于存储其本身密钥信息的解密算法程序，一个ROM 14，用于存储其本身的密钥信息，和一个RAM 15，用于临时存储另一个智能卡的密钥信息，和一个处理器11，用于相对于ROM 14或RAM 15中存储的密钥信息通过第一和第二算法存储存储器12和13的存储算法的进行加密或解密。

当时，处理器11和16可以通过逻辑布线构成或可以采用一个微处理器。在采用微处理器的情况下，程序中可以加入用于智能卡的加密算法。

现在将描述具有如上所述结构的本发明的操作和效果。

在本发明中，GA比特流被以图11A到11C所示的格式传输，其中图11A示出未扰频格式，图11B示出相对于比特流的扰频格式，图11C示出比特流被有选择地扰频的格式。

在本发明中，如果GA比特流被扰频，则假设其可适用于任何种类的保护。

因此，如果图11B或11C所示格式的被扰频流数据$S_{KS}(BS) + E^{Q}(KS)$输入到复制保护处理器4，一个图10所示的分离器将该流数据分离成比特流$S_{KS}(BS)$ + IDX和密钥流$E^{Q}(KS)$。此后，执行一种记录方式再次对被分离密钥流$E^{Q}(KS)$加密，然后传输到智能卡3。

在这里，如图11C所示，如果比特流被部分地扰频，防止非法

收看和复制的功能仅适用于扰频部分，因此只能执行部分保护功能。

首先，当未扰频比特流如图11A所示传输时，即使在解调器&误差校正器1中被调制/解调和解密的比特流输入到复制保护处理器4，数据也不传输到智能卡3。而且，ATV解码器2不将从解调器&误差校正器1输入的比特流传输到智能卡3，但对该比特流解密。

因此，对收看和复制没有限制。

在这里，从调谐器输入到解调器&误差校正器1的信号和从ATV解码器2输出的视频和音频信号是模拟信号。从调谐器输出的信号是来自GA-比特流的VSB调制信号。

在输入/输出信号之中，比特流和密钥流是用于DVCR的数字信号。

当时，如果进行记录，将比特流记录到DVCR上，并且所记录的比特流从一个普通DVCR播放。

换句话说，即使未扰频的MPEG比特流被输入到复制保护处理器4并通过图10所示的分离器，由于无密钥信息，数据不传输到智能卡3，因此允许自由收看和复制。

另外，当在本发明中执行记录或复制保护功能时，被分离的比特流和密钥流被传输到相互不同的线路。按传输的信息通过PES标题中的附加复制信息字段传输与复制保护方法有关的信息。

当时，即使具有不被加密密钥的被扰频比特流传输到公用信道的非法用户，在除去密钥信息的状态下不能正常地执行解扰。

另外，被分离的密钥再次被加密传输。因此，如果没有解密算法，不能解扰比特流。

因此，在本发明中，为防止非法收看和复制，在MPEG传输协议

中使用一个任意字段，其中被进行扰频的比特流采用复制保护功能。

首先，如果传输扰频控制字段变成“未扰频”方式，ATV解码器2不进行解扰，以使非法用户不能操作该字段。

在这种复制保护方法中，复制保护或自由复制功能由传输扰频控制字段确定。因此，非法用户仅通过处理该字段不能解除复制保护功能。

接下来，非法用户可以改变PES标题中的附加复制信息字段来转换保护方法。该方法并未消除保护方法本身，对复制保护功能不造成显著破坏。

由具有上述特性的本发明支持的复制保护方法包括“禁止复制”方法，“复制前付费(PPC)”方法，和具有收看前付费(PPV)功能和播放前付费(PPP)功能缺省的“备份复制”方法。

在这里，“禁止复制”方法使其很难被另一盘录像带复制。“PPC”方法是指每一次复制前付费。“备份复制”方法允许从第一DVCR播放并从第二DVCR复制的录像带只能在第一DVCR中正常显示，而不能在第二DVCR中正常显示。

现在将参考图19至21描述根据本发明的复制保护方法和对应MPEG比特流的流程。

在这里，图19示出记录或播放状态期间复制保护处理器操作的信号流程，图20示出智能卡与复制保护处理器对应的操作信号流程，图21示出记录和重现操作期间用于密钥交换和鉴别的信号流程。

首先，参考图19A，复制保护处理器4校验输入的比特流是否存在密钥信息，以确定密钥信息是否被扰频，如果密钥信息被扰频(S101)确定该记录是否是第一次记录或复制记录。换句话说，在被

扰频数据的情况下，检测是否是通过将该数据分离成比特流S_{KS}(BS)和密钥流E^{G}(KS)以S_{KS}(BS) + IDX格式的流来传输该数据。 如果检测到S_{KS}(BS) + IDX格式流，则确定该记录为复制记录。 如果未检测到，则确定该记录为第一次记录(S102)。

因此，如果确定该记录为第一次记录，将比特流和密钥流混合的流S_{KS}(BS) + E^{G}(KS)记录到录像带上(S106)。如果确定该记录是复制记录， 与密钥流E^{G}(KS)分离的比特流S_{KS}(BS) + IDX被传输到记录一侧的复制保护处理器8，并相对于密钥信息AK再次对密钥流E^{G}(KS)加密(S105)。然后，经智能卡3将被加密密钥流E_{SC}^{AK}[E^{G}(KS)]传输到记录一侧的智能卡7， 从而允许将其记录在记录一侧VCR9中的录像带上(S106)。

与此相反，图19B示出了在播放用图19A所示的同样的信号流程记录的录像带情况下的信号流程， 其中如果输入从VCR播放的比特流(S107)，复制保护处理器4分离和确定密钥流(S108)， 从而确定记录功能是否是“备份记录”(S110)。

此时，在步骤S110中，如果没有密钥信息，则确定该录像带为普通录像带，如果检测到被加密的密钥流E^{G}(KS)，则确定该录像带为第一次录像带。另外，如果密钥流D_{SC}^{AK}[E^{G}(KS)]被相对于其本身密钥信息AK加密，则确定该录像带为PPC功能录像带。 如果密钥流D_{SC}^{AL}[E^{G}(KS)]被相对于另一个智能卡的密钥信息AL加密，则确定该录像带为备份复制功能录像带。

因此，在普通录像带情况下，复制保护处理器4将该比特流(BS)传输到ATV解码器2，并在备份复制功能录像带的情况下将比特流S_{KS}(BS) + IDX与密钥流E^{G}(KS)分离(S109)。

复制保护功能录像带的播放期间，如果采用备份复制功能，复制保护处理器4将相对于其本身的密钥信息AK用加密算法$E^{SC}_{AK}(.)$加密两次的被加密密钥流$D_{SC}^{AK}[E^{G}(KS)]$传输到智能卡3(S111，S112和S113)。另外，如果未采用备份复制功能，复制保护处理器4将用加密算法$E^{SC}_{AK}(.)$通过加密密钥流$E^{G}(KS)$获取的被加密密钥流$E_{SC}^{AK}[E^{G}(KS)]$传输到智能卡3(S112和S113)。

在复制保护处理器4进行上述操作的同时，智能卡3进行如图20所示的操作。详述如下，通过进行广播或播放操作，智能卡3确定是否从ATV解码器2输入索引码IDX或密钥流$E^{G}(KS)$(S114和S115)。

当时，如果输入的是密钥流$E^{G}(KS)$而不是索引码IDX，已经确定PPV功能广播收看的智能卡3相对于比特流GA用解密算法$D^{G}(.)$对密钥流$E^{G}(KS)$解密(S116)，并将密钥信息KS输入到ATV解码器2(S117)。

因此，ATV解码器2读取智能卡3的密钥信息KS，确定一种解扰方法并解扰比特流$S_{KS}(BS)$，输出模拟视频和音频信号，从而允许观众观看广播节目。

如果确定在S115输入的是索引码IDX，智能卡3相对于密钥信息AK用解密算法$D^{SC}_{AK})(.)$对从复制保护处理器4输入的密钥流$E_{SC}^{AK}[E^{G}(KS)]$解密(S118)，然后确定该操作是否是播放操作或记录操作(S119)。

当时，如果确定S119中的操作是播放操作，智能卡3相对于比特流GA用解密算法$D^{G}(.)$(S116)对密钥流$E^{G}(KS)$解密(S116)并将密钥信息KS输入到ATV解码器2(S117)。

因此，ATV解码器2读取智能卡3的密钥信息KS，确定一种解扰方法并通过确定的解扰方法将在复制保护处理器4中分离的比特流

S_{KS}(BK)解扰，以输出模拟视频和音频信号，从而允许观众观看录像带记录的节目。

如果确定S119中的操作是记录操作，智能卡3确定该功能是否是备份复制功能(S120)。如果该功能是备份复制功能，相对于密钥信息AK用解密算法$D^{SC}_{AK}(.)$对密钥流E^{G}(KS)解密(S121)，然后相对于密钥信息AL用解密算法$D^{SC}_{AK}(.)$对密钥流$D^{SC}_{AK}[E^{G}(KS)]$解密(S122)。

当时，将在智能卡3中被解密的密钥流$D^{SC}_{AK}\{D^{SC}_{AL}[E^{G}(KS)]\}$传输到记录一侧(S123)并通过智能卡7输入到复制保护处理器8(S124)，然后用加密算法$E^{SC}_{AL}(.)$加密。

因此，智能卡7将该加密密钥流$D^{SC}_{AK}[E^{G}(KS)]$插入由索引码指定的位置并将其与播放一侧的复制保护处理器4输出的比特流S_{KS}(BS)混合，然后记录在VCR9中的录像带上。

如果确定S119中的操作是记录操作，并在S120确定是采用PPP功能而不是备份复制功能，智能卡3相对于密钥信息AL用解密a算法$D^{SC}_{Al}(.)$对密钥流E^{G}(KS)解密(S122)，并将被解密的密钥信息$D^{SC}_{AL}[E^{G}$(KS)]传输到记录一侧(S123)。

当时，记录一侧的复制保护处理器8已经通过智能卡7接收密钥$D_{SC}^{AL}[E^{G}(KS)]$，复制保护处理器8用加密算法$E^{SC}_{Al}(.)$对接收的密钥$D_{SC}^{AL}[E^{G}$(KS)]加密并将被加密密钥流$[E^{G}(KS)]$插入由索引码IDX指定的位置，从而与播放一侧的复制保护处理器4输出的比特流S_{KS}(BS)混合。因此，从复制保护处理器8输出的比特流$S_{KS}(BS) + E^{G}(KS)$由VCR9记录到录像带上。

如上所述，在本发明中，所有智能卡对于MPEG比特流具有相对于加密算法$E^{G}(.)$和解密算法$D^{G}(.)$的公共算法和公共密钥。

另外，用于一个智能卡的加密算法$E^{SC}_{AI}(.)$和解密算法$S^{SC}_{AK}(.)$对所有智能卡都是公共的。但各个智能卡的密钥信息不同。

换句话说，每个智能卡自身中包含与其本身识别(ID)相对应的鉴别密钥。

在该操作中，初始化必须包括识别复制保护处理器和智能卡之间，以及智能卡和密钥交换处理之间的正副本的鉴别过程。

当时，作为鉴别过程，已经提出了许多方法，例如使用类似DES算法的对称密钥算法的方法，使用类似RSA的公用密钥算法的方法，或使用Fiat－Shamir(FS)的方法方案。

在本发明中，鉴别过程中使用公用密钥算法并且其密钥交换方法在图21中示出。以密钥接收装置201和密钥传输装置202共享公用密钥(n, e)为基础采用该方法。

当时，密钥接收装置201是记录一侧的一个复制保护处理器或一个智能卡1，传输装置202是其本身的智能卡k。

下面将参考图12至18描述上面流程图中所示的本发明操作的实施例。

如图11A所示，在本发明中，如果传输未扰频比特流BS，电路工作如图12所示。因此，在解调器&误差校正器1中被调制/解调和RS-解码的比特流在ATV解码器2中被解密，然后输出模拟视频和音频信号。

当时，记录操作过程中，从解调器&误差校正器1输出的比特流BS通过复制保护处理器4记录在VCR5中的录像带上。重现操作过程中，从VCR5播放的比特流BS通过复制保护处理器4输入到ATV解码器2并被解密，然后输出模拟视频和音频信号。

换句话说，由于数据不是从复制保护处理器4产生输入到智能卡3，因此收看和复制不受影响。

如图11B和11C，如果输入被扰频比特流，所采用的CA功能进行图13至18所示的操作。

首先，在执行PPV功能的情况下，电路操作如图13所示。也就是说，如果传输被扰频比特流S_{KS}(BS)和被加密密钥流E^{G}(KS)，解调器&误差校正器1解调被调制的输入信号并通过RS-解码校正传输期间产生的误差。

当时，ATV解码器2分离解调器&误差校正器1的输出S_{KS}(BS) + E^{G}(KS)中分离密钥流E^{G}(KS)并将其输出到智能卡3。然后，智能卡3对被加密的密钥流E^{G}(KS)解密并再次将密钥流KS输出到ATV解码器2。

因此，ATV解码器2读取智能卡3的密钥信息KS，确定一种解扰方法并对比特流S_{KS}(BS)解扰输出模拟视频和音频信号。

如上所述，图9所示的智能卡3允许处理器11对被加密的密钥流E^{G}(KS)解密并通过解密算法E^{G}(.)将被解密的密钥流KS输出到ATV解码器2。

在第一次记录被扰频比特流的情况下，电路操作如图14所示，其中传输的比特流S_{KS}(BS) + E^{G}(KS)在解调器&误差校正器1中通过RS解码校正误差然后通过复制保护处理器4输入到VCR5记录在录像带上。

在播放如上所述记录的比特流的情况下，如果该功能是PPP功能，该系统如图15所示操作。如果从VCR5播放的比特流S_{KS}(BS) + E^{G}(KS)输入到复制保护处理器4，复制保护处理器4将播放的比特流S_{KS}(BS) + E^{G}(KS)分离成比特流S_{KS}(BS)和密钥流E^{G}(KS)，然后再次用加

密算法$E^{SC}_{AK}(.)$对分离的密钥流$E^{G}(KS)$加密，将其输出到智能卡3。将被取出密钥流$E^{G}(KS)$部分的分离比特流$S_{KS}(BS)$中插入索引码IDX输出到ATV解码器2。

当时，已经通过ATV解码器2接收索引码IDX的智能卡3用用于智能卡的解密算法$D^{SC}_{AK}(.)$对复制保护处理器2的被加密密钥流$E_{AK}^{SC}[E^{G}(KS)]$解密，并将密钥流(解扰信息)KS输出到ATV解码器2(S117)。

因此，ATV解码器2读取智能卡3的密钥流KS，确定解扰方法，并对经复制保护处理器4输入的比特流$S_{KS}(BS)$解密，从而输出模拟视频和音频信号。

另外，在将如图14所示记录的数据记录在不同的VCR上的情况下，如图16所示执行PPC功能。如果从VCR5播放的比特流$S_{KS}(BS) + E^{G}(KS)$输入到复制保护处理器4，复制保护处理器4将播放的比特流$S_{KS}(BS) + E^{G}(KS)$分离成比特流$S_{KS}(BS)$和密钥流$E^{G}(KS)$，然后再次用加密算法$E^{SC}_{AK}(.)$对分离的密钥流$E^{G}(KS)$加密，将其输出智能卡3。将被取出密钥流$E^{G}(KS)$部分的分离比特流$S_{KS}(BS)$中插入索引码IDX输出到记录一侧的复制保护处理器8。

当时，播放一侧的智能卡3根据存储在RAM15中的密钥信息AL用解密算法$D^{SC}_{AL}(.)$对复制保护处理器4中的被加密的密钥流$E^{SC}_{AK}[E^{G}(KS)]$解密，并将被解密的密钥流$D^{SC}_{AL}[E^{G}(KS)]$输出到记录一侧的智能卡7。

因此，如果记录一侧的智能卡7接收播放一侧智能卡3的密钥流$D^{SC}_{AL}[E^{G}(KS)]$并将其输出到复制保护处理器8，复制保护处理器8对密钥流$D^{SC}_{AL}[E^{G}(KS)]$加密并将其恢复成原始被加密密钥流$E^{G}(KS)$，即该密钥流$E^{G}(KS)$根据索引码IDX与播放一侧的复制保护处理器4输出的比特流$G_{KS}(BS)$混合输出到VCR9，从而将其记录在另一盘录像带上。

以上所述操作记录的录像带数据采用PPP功能并如图15所示播放。

另外，在将如图14所示记录的数据记录在另一个VCR上的情况下，如图17所示执行备份复制功能。

换句话说，如果从VCR5播放的比特流$S_{KS}(BS)+E^{G}(KS)$输入到复制保护处理器4，复制保护处理器4将播放的比特流$S_{KS}(BS)+E^{G}(KS)$分离成比特流$S_{KS}(BS)$和密钥流$E^{G}(KS)$，然后再次用加密算法$E_{AK}^{SC}(.)$对分离的密钥流$E^{G}(KS)$加密，将其输出到智能卡3。将被取出密钥流$E^{G}(KS)$部分的分离比特流$S_{KS}(BS)$中插入索引码IDX输出到记录一侧的复制保护处理器8。

当时，播放一侧的智能卡3相对于存储在ROM14中其本身的密钥信息AK用解密算法$D^{SC}_{A1}(.)$对在复制保护处理器4中被加密的密钥流$E^{SC}_{AK}[E^{G}(KS)]$解密两次，并相对于存储在RAM15中的密钥信息A1用解密算法$D^{SC}_{A1}(.)$对其再次解密，然后将被解密的密钥流$D^{SC}_{A1}\{D^{SC}_{AK}[E^{G}(KS)]\}$输出到记录一侧的智能卡7。

因此，如果播放一侧的智能卡3的密钥流$D^{SC}_{A1}\{D^{SC}_{AK}[E^{G}(KS)]\}$通过记录一侧的智能卡7输出到记录一侧的复制保护处理器8，复制保护处理器8相对于密钥信息AL加密密钥流$D^{SC}_{A1}\{D^{SC}_{AK}[E^{G}(KS)]\}$并将其恢复成原始被加密密钥流$D^{SC}_{AK}[E^{G}(KS)]$。被恢复的$D_{AK}^{SC}[E^{G}(KS)]$根据索引码IDX与播放一侧的复制保护处理器4输出的比特流$G_{KS}(BS)$混合输出到VCR9，从而将其记录在另一个录像带上。

在这里，在改进的智能卡3或7中计算收费。

通过执行备份复制功能记录的数据只能从记录原始录像带的VCR播放。在正常播放的情况下，如图18A所示执行该操作。

换句话说，如果从VCR5播放的比特流$S_{KS}(BS)+D^{SC}_{AK}[E^{G}(KS)]$输入到

复制保护处理器4，复制保护处理器4将该比特流$S_{KS}(BS) + D^{SC}_{AK}[E^{G}(KS)]$分离成比特流$S_{KS}(BS)$和密钥流$D^{SC}_{AK}[E^{G}(KS)]$，然后用加密算法$E^{SC}_{AK}(.)$对被分离的密钥流$D^{SC}_{AK}[E^{G}(KS)]$再次加密两次，将其输出到智能卡3。将被取出密钥流$D^{SC}_{AK}[E^{G}(KS)]$部分的分离比特流$S_{KS}(BS)$中被插入索引码IDX输出到ATV解码器2。

当时，已经通过ATV解码器2接收索引码IDX的智能卡3用智能卡的解密算法$D^{SC}_{AK}(.)$对在复制保护处理器2中被加密的密钥流$E^{SC}_{AK}[E^{G}(KS)]$解密两次，并将密钥流(解扰信息)KS输出到ATV解码器2。

因此，ATV解码器2读取智能卡3的密钥流KS，确定解扰方法，并对经复制保护处理器4输入的比特流$S_{KS}(BS)$解密，从而输出模拟视频和音频信号。

另外，在不是原始记录VCR的另一个VCR非正常播放的情况下，执行如图18B所示的操作，从而使录像带的播放无效。

换句话说，如果被复制的录像带是从已经执行录像带复制的VCR播放，复制保护处理器8将播放数据$S_{KS}(BS) + D^{SC}[E^{G}(KS)]$分离成比特流$S_{KS}(BS) + IDX$。

当时，被分离的比特流$D^{SC}_{AK}[E^{G}(KS)]$被相对于其本身的密钥信息AL加密，并且相对于密钥信息AL再次被加密变成$E^{SC}_{AL}\{E^{SC}_{AL}[D^{SC}_{AK}[E^{G}(KS)]$，然后传输到智能卡7。

当时，智能卡7不能对密钥流$E^{SC}_{AL}\{E^{SC}_{AL}(D^{SC}_{AK}[E^{G}(KS)]\}$解密，使密钥信息KS不能被传输到ATV解码器6。

因此，智能卡7不能解扰比特流$S_{KS}(BS)$，使复制的录像带不能播放。

如上所述，根据本发明，由于鉴别和密钥交换过程是在通电或

DVCR之间连接期间自动进行的，能够自动执行防止非法智能卡的非法收看和复制功能。另外，由于能够部分地执行防止非法收看和复制，可以根据节目所需保护的部分进行扰频过程，从而自动执行防止非法收看和复制并能按所需方式收费。

另外，在本发明中，由于被分离的比特流和密钥流输到不同路径，能够减少保护数据的数量，从而有效地进行防止非法收看和复制。 在以智能卡实现防止非法收看和非法复制的保护中， 区分为PPV、PPP、PPC和备份复制功能，从而对对应的功能区别收费。

根据本发明，用于数字信号的复制保护可适用于DSM应用， 允许用于DSM，例如DVCR的节目版权保护。 从而使防止非法收看和复制的可靠性增加。

最后，为便于理解本发明，本规定中使用的术语定义如下:

1) BS: 未被扰频的GA比特流;

2) $KS = [K_0, K_1, K_2 \ldots\ldots K_i \ldots\ldots K_n]$: 密钥流(在这里，n是用于扰频的密钥总数);

3) $BS = [BS_0, BS_1, BS_2 \ldots\ldots BS_i \ldots\ldots BS_n]$: 比特流(在这里，$BS_i$是BS的一段并且是一个扰频单元);

4) $S_{KS}(BS) = [S_{K0}(BS_0), S_{K1}(BS_1), S_{K2}(BS_2) \ldots\ldots S_{Ki}(BS_i) \ldots\ldots S_{Kn}(BS_n)]$: 被扰频GA比特流;

5) E(.) & D(.): GA中用于密钥加密和解密的算法;

$E^G(KS) = [E^G(K_0), E_G(K_1), E^G(K_2) \ldots\ldots E^G(K_i) \ldots\ldots E^G(K_n)]$和

$D^G[E^G(KS)] = [D^G[E^G(K_0)], D^G[E_G(K_1)], D^G[E^G(K_2)] \ldots\ldots$

$D^G[E^G(K_i)] \ldots\ldots D^G[E^G(K_n)]] = KS$;

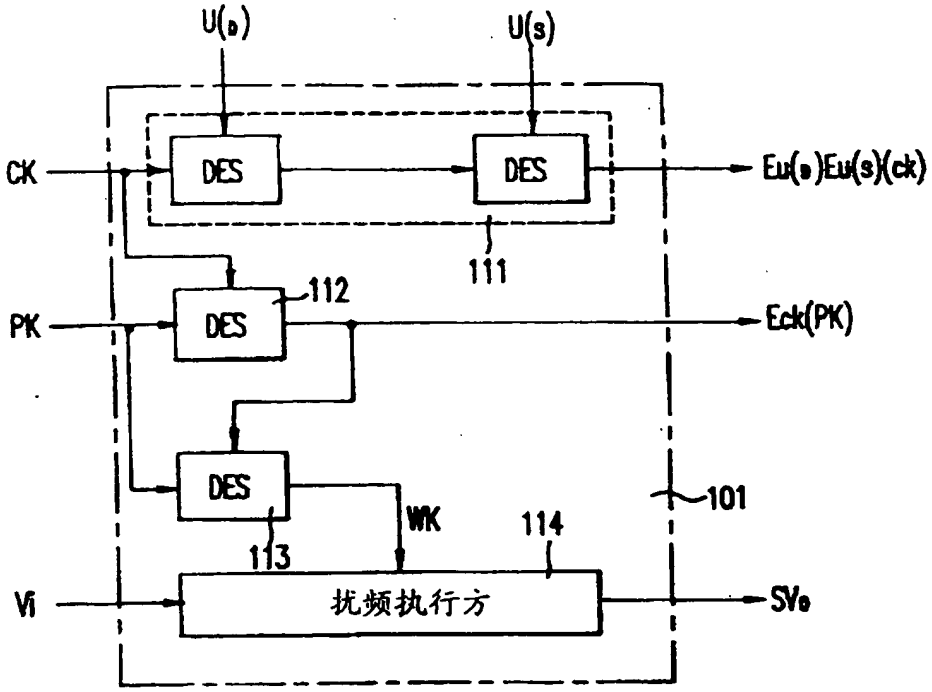
6) IDX=[0, 1, 2, ……i, ……n]: 索引流;

7) AK: 用于智能卡(K)的鉴别密钥; 和

8) $E^{sc}_{A}(.)$ & $D^{sc}_{A}(.)$: 用智能卡鉴别密钥(A)作为智能卡的加密和解密算法。

说 明 书 附 图

图 1



DEC: 数据加密标准

图 2

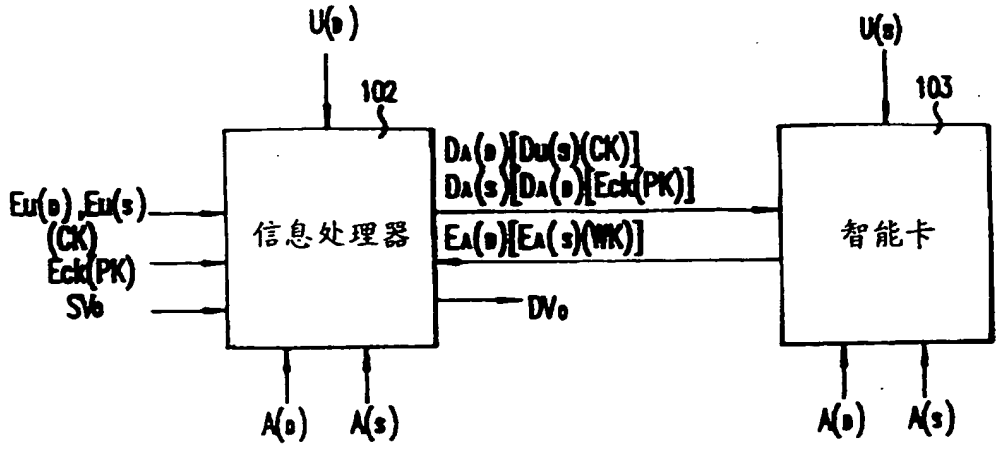


图 3

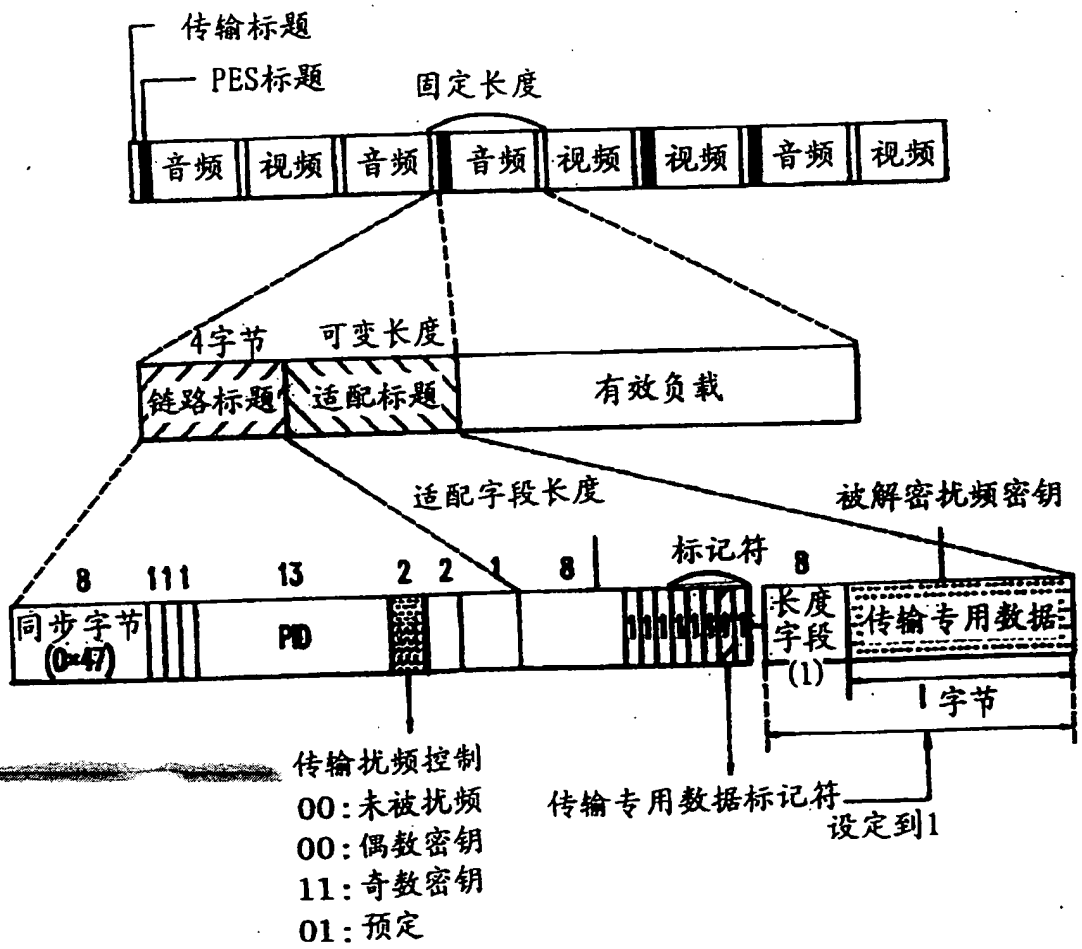

传输标题
PES标题
固定长度
音频
视频
音频
音频
视频
视频
音频
视频
4字节
可变长度
链路标题
适配标题
有效负载
适配字段长度
被解密扰频密钥
标记符
8
111
13
2
2
1
8
8
同步字节
(0x47)
PID
长度
字段
(1)
传输专用数据
1字节
传输扰频控制
00：未被扰频
00：偶数密钥
11：奇数密钥
01：预定
传输专用数据标记符
设定到1

图 4

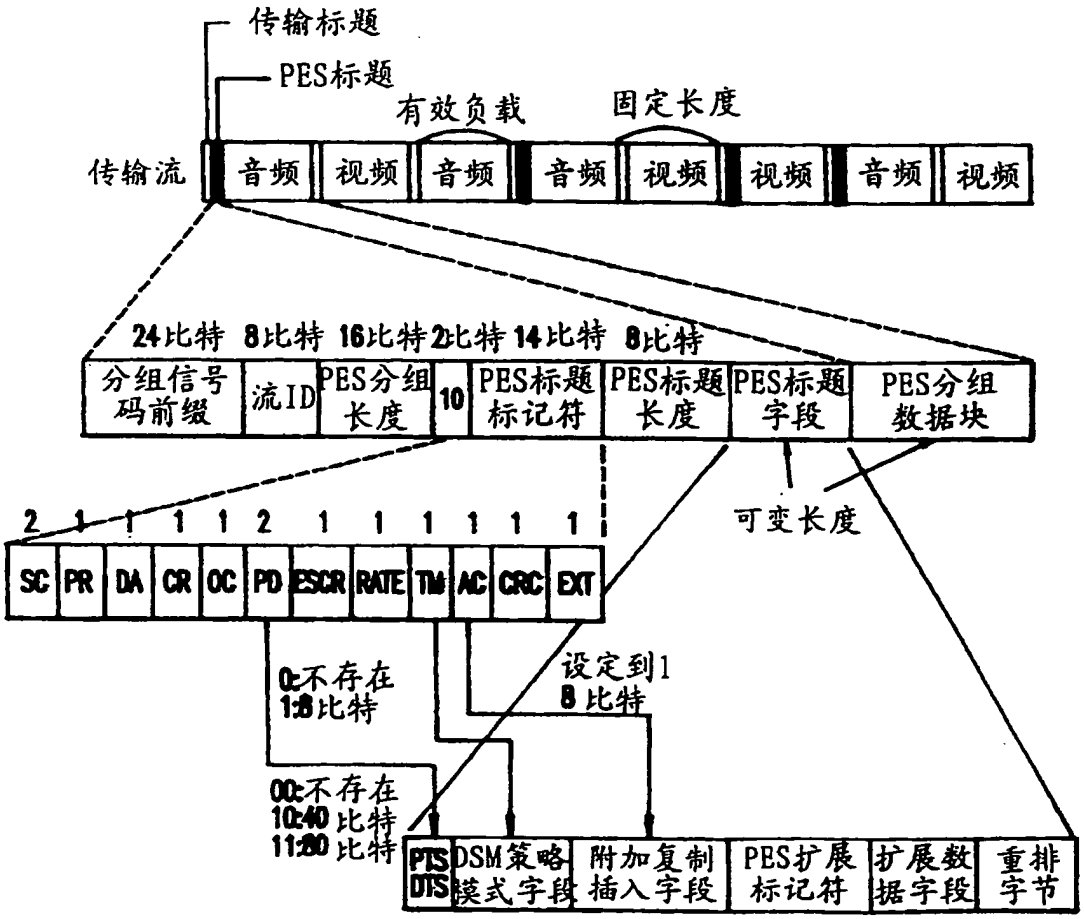

传输标题
PES标题
有效负载
固定长度
传输流
音频
视频
音频
音频
视频
视频
音频
视频
24比特
8比特
16比特
2比特
14比特
8比特
分组信号码前缀
流ID
PES分组长度
10
PES标题标记符
PES标题长度
PES标题字段
PES分组数据块
可变长度
2
1
1
1
1
2
1
1
1
1
1
1
SC
PR
DA
CR
OC
PD
ESCR
RATE
TM
AC
CRC
EXT
0:不存在
1:5比特
设定到1
8比特
00:不存在
10:40比特
11:80比特
PTS
DTS
DSM策略模式字段
附加复制插入字段
PES扩展标记符
扩展数据字段
重排字节

图 5

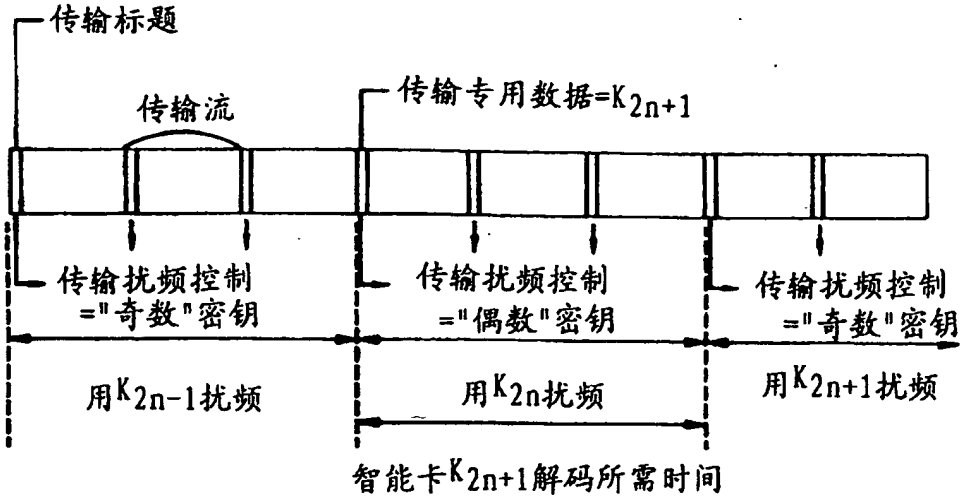

传输标题
传输流
传输专用数据=K2n+1
传输扰频控制
="奇数"密钥
传输扰频控制
="偶数"密钥
传输扰频控制
="奇数"密钥
用K2n-1扰频
用K2n扰频
用K2n+1扰频
智能卡K2n+1解码所需时间

图 6

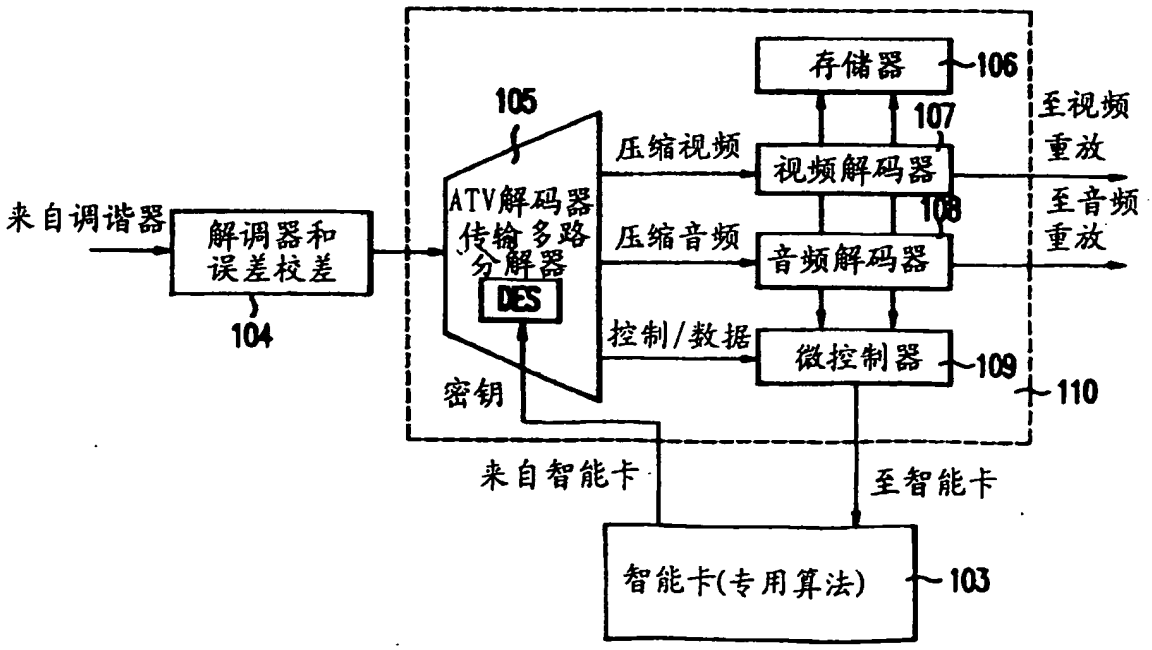

来自调谐器
解调器和
误差校差
104
105
ATV解码器
传输多路
分解器
DES
密钥
压缩视频
压缩音频
控制/数据
存储器
106
107
视频解码器
108
音频解码器
微控制器
109
110
至视频
重放
至音频
重放
来自智能卡
至智能卡
智能卡(专用算法)
103

图 7

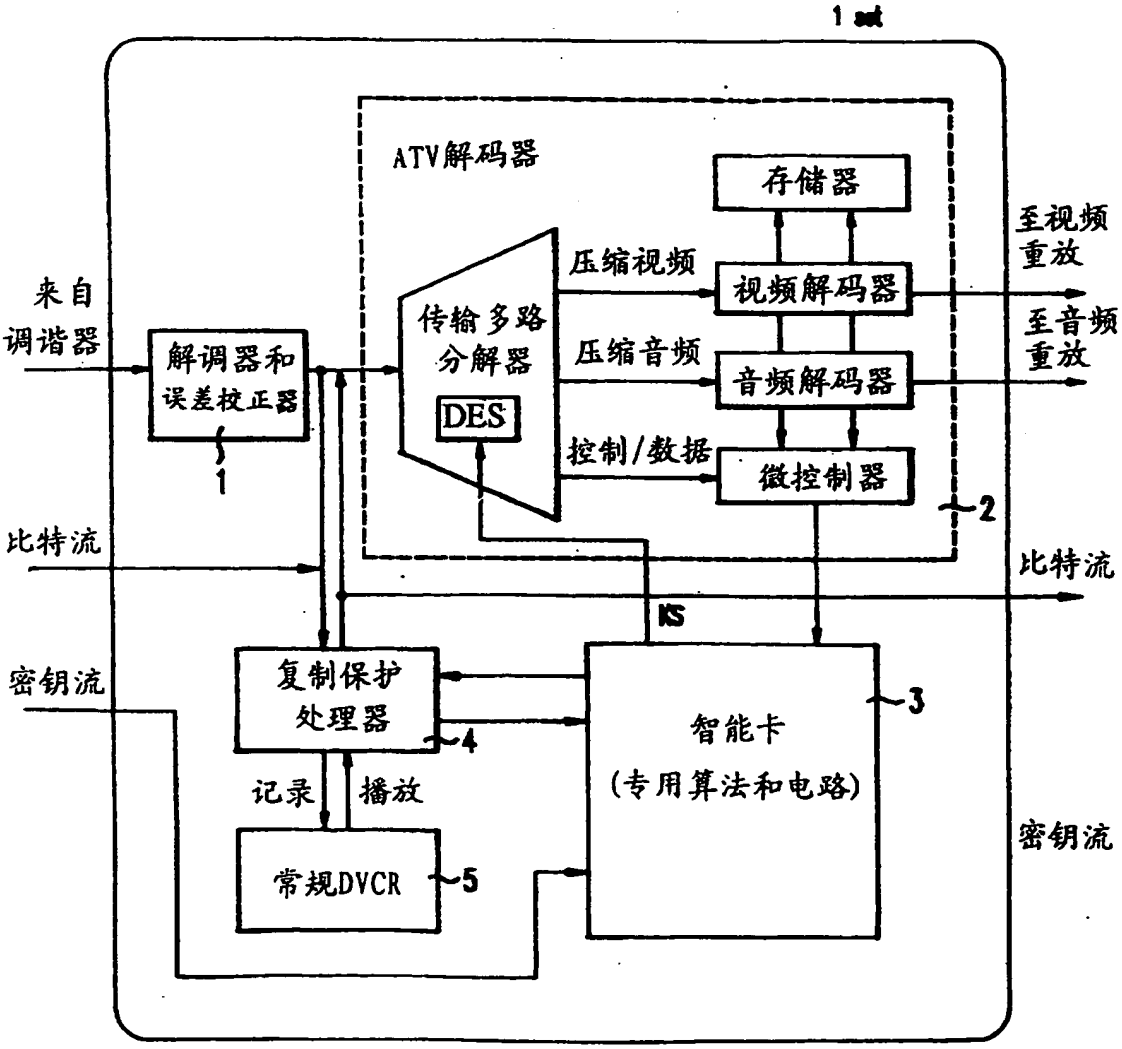

ATV解码器
存储器
压缩视频
视频解码器
至视频重放
来自调谐器
传输多路分解器
DES
压缩音频
音频解码器
至音频重放
解调器和误差校正器
1
控制/数据
微控制器
2
比特流
比特流
KS
密钥流
复制保护处理器
4
智能卡
(专用算法和电路)
3
记录
播放
常规DVCR
5
密钥流

图 8

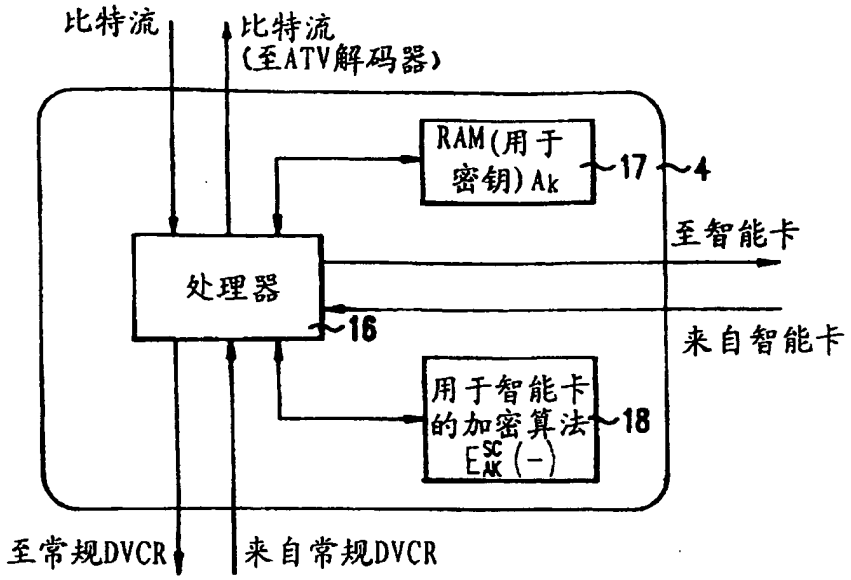

比特流
比特流
(至ATV解码器)
RAM(用于
密钥) Ak
17
4
至智能卡
处理器
16
来自智能卡
用于智能卡
的加密算法
$E^{SC}_{AK}(-)$
18
至常规DVCR
来自常规DVCR

图 9

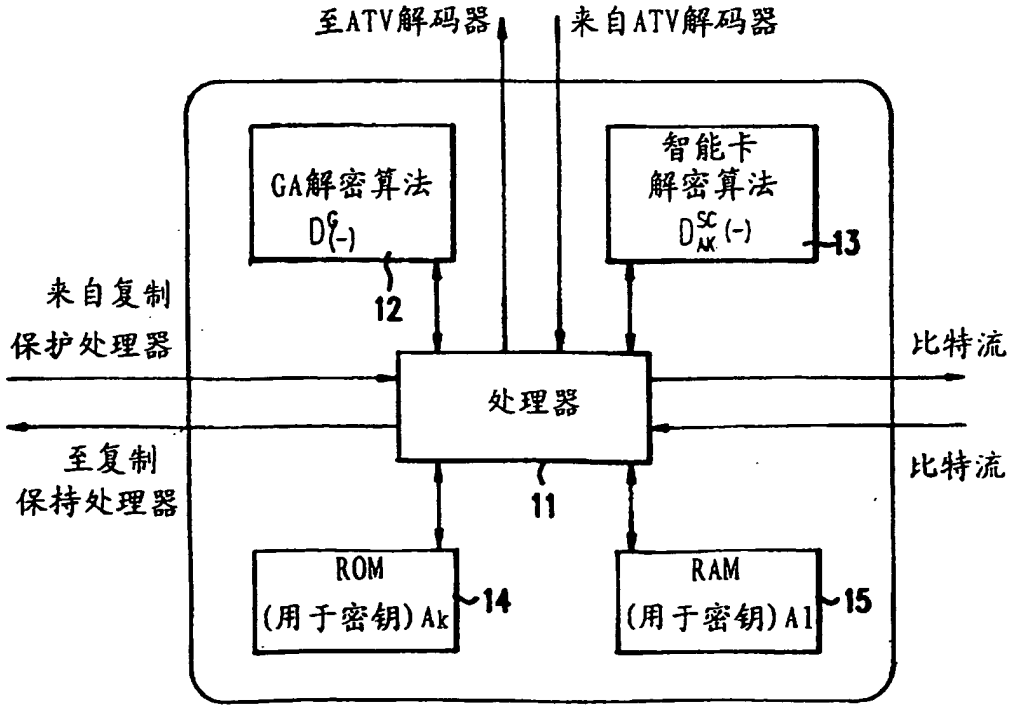

至ATV解码器
来自ATV解码器
GA解密算法
$D^{G}(-)$
智能卡
解密算法
$D^{SC}_{AK}(-)$
13
12
来自复制
保护处理器
比特流
处理器
至复制
保持处理器
比特流
11
ROM
(用于密钥) Ak
14
RAM
(用于密钥) A1
15

图 10

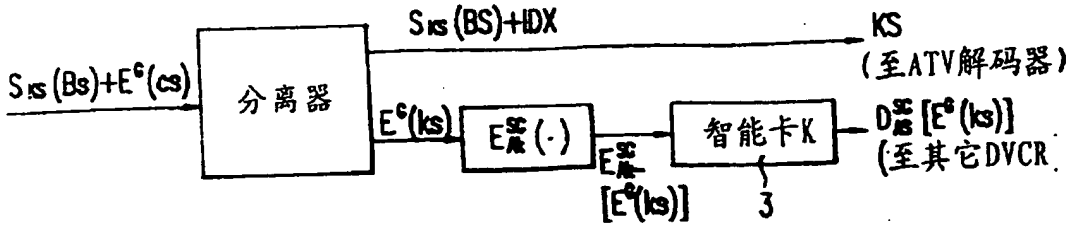


图 11 a

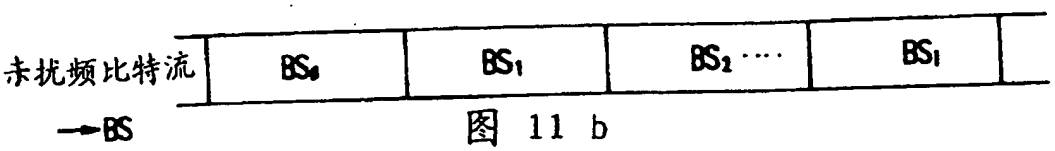


图 11 b

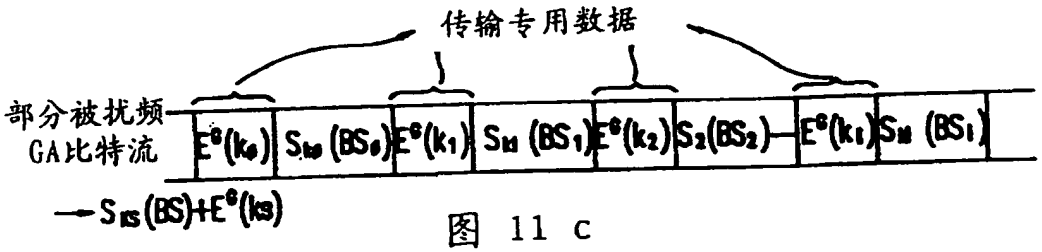


图 11 c

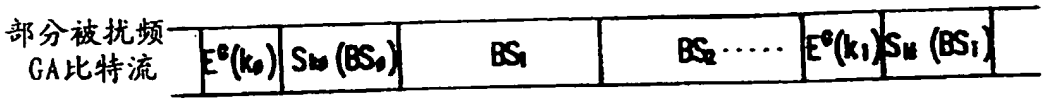


图 11 d

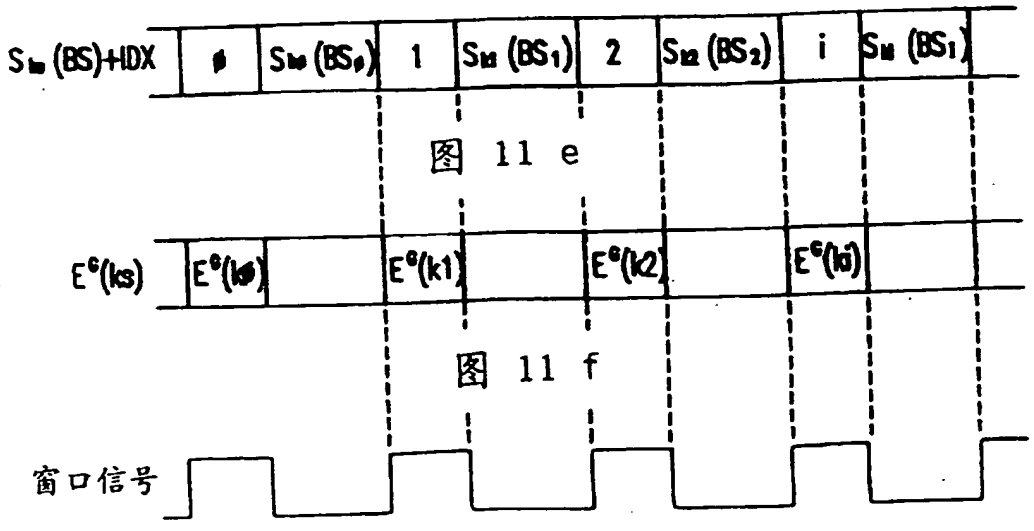


图 11 e

图 11 f

图 12

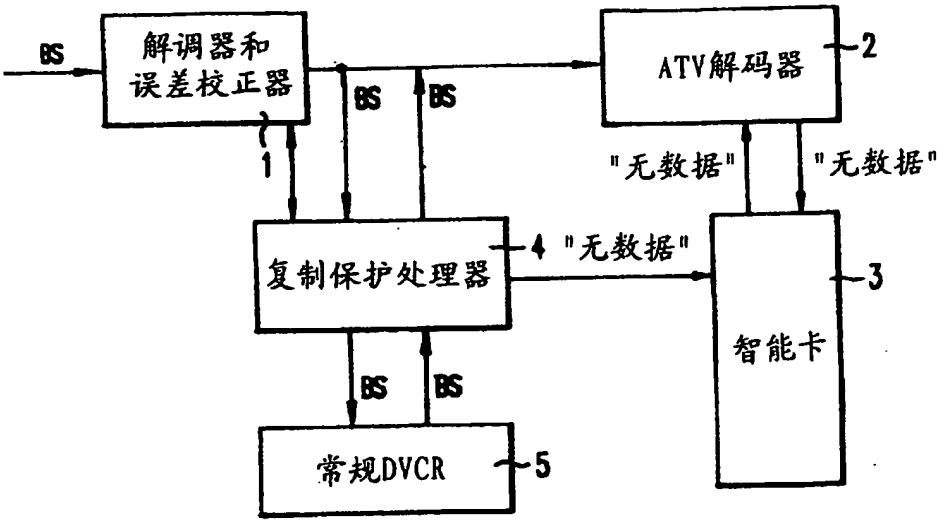

BS
解调器和
误差校正器
1
BS
BS
ATV解码器
2
"无数据"
"无数据"
复制保护处理器
4
"无数据"
3
智能卡
BS
BS
常规DVCR
5

图 13

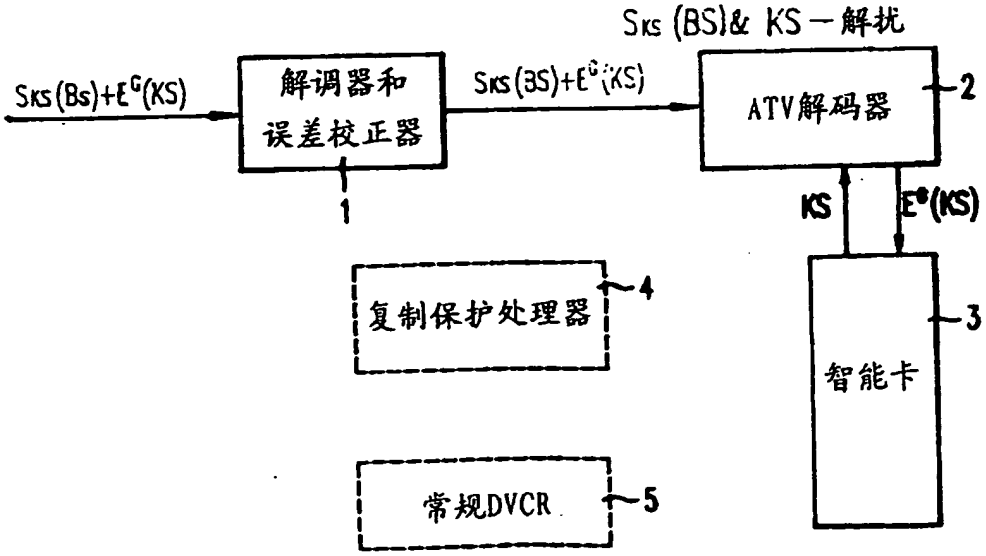

SKS (BS)& KS－解扰
SKS(Bs)+E^G(KS)
解调器和
误差校正器
SKS(BS)+E^G(KS)
ATV解码器
2
1
KS
E^G(KS)
复制保护处理器
4
3
智能卡
常规DVCR
5

图 14

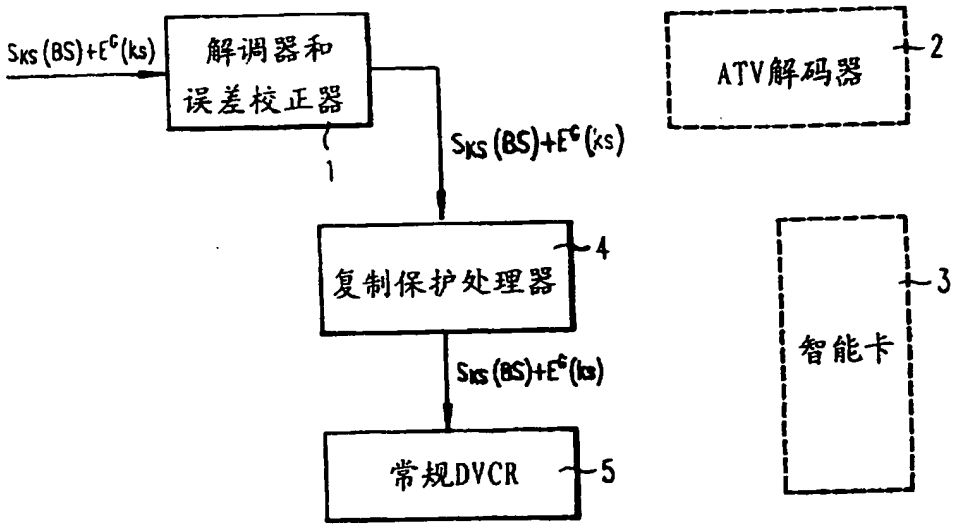

$S_{KS}(BS)+E^{G}(ks)$
解调器和
误差校正器
1
$S_{KS}(BS)+E^{G}(ks)$
ATV解码器
2
复制保护处理器
4
$S_{KS}(BS)+E^{G}(ks)$
智能卡
3
常规DVCR
5

图 15

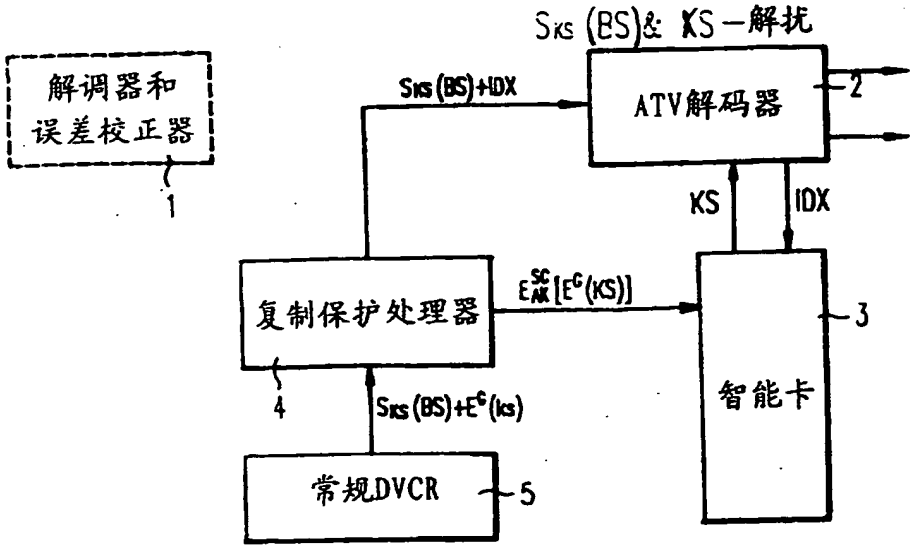

$S_{KS}(BS)$& KS—解扰
解调器和
误差校正器
1
$S_{KS}(BS)$+IDX
ATV解码器
2
KS
IDX
复制保护处理器
$E^{SC}_{AK}[E^{G}(KS)]$
3
智能卡
4
$S_{KS}(BS)+E^{G}(ks)$
常规DVCR
5

图 16

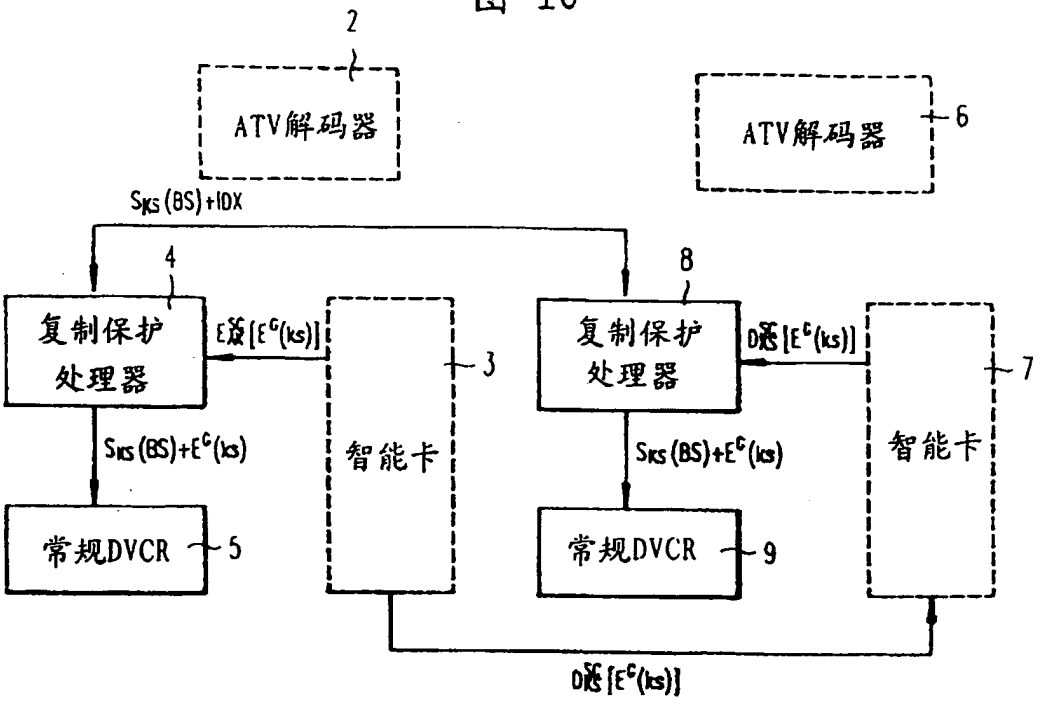

2
ATV解码器
ATV解码器
6
SKS(BS)+IDX
4
8
复制保护处理器
复制保护处理器
3
7
常规DVCR
5
常规DVCR
9
智能卡
智能卡

图 17

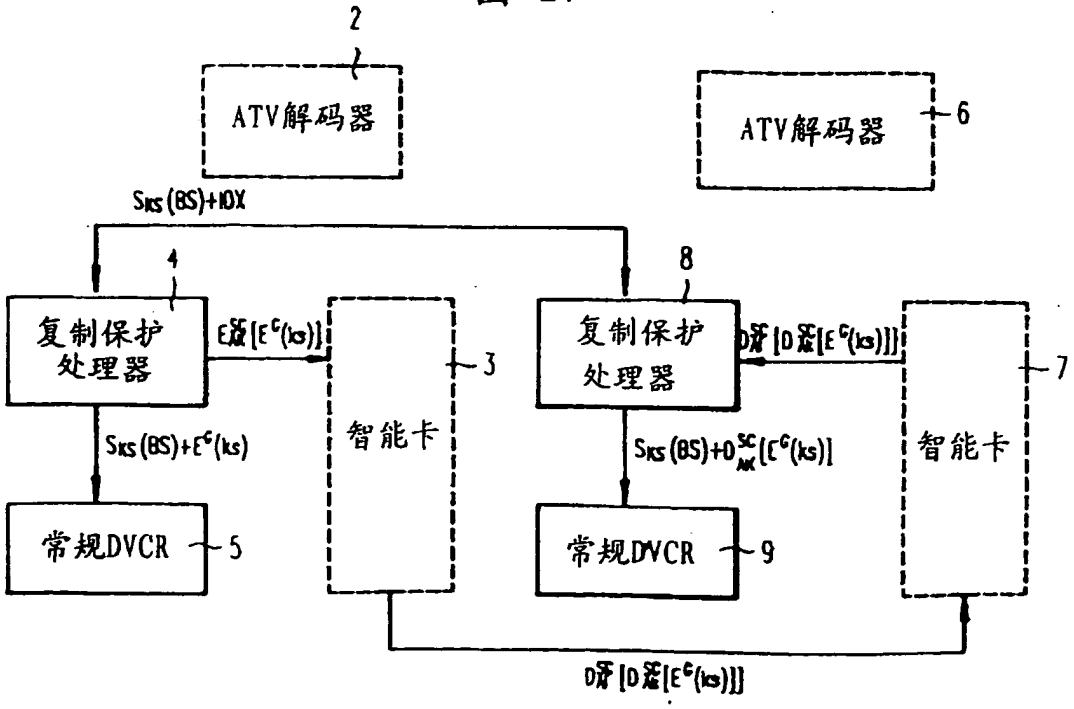

2
ATV解码器
ATV解码器
6
SKS(BS)+IDX
4
8
复制保护处理器
复制保护处理器
3
7
常规DVCR
5
常规DVCR
9
智能卡
智能卡

图 18 a

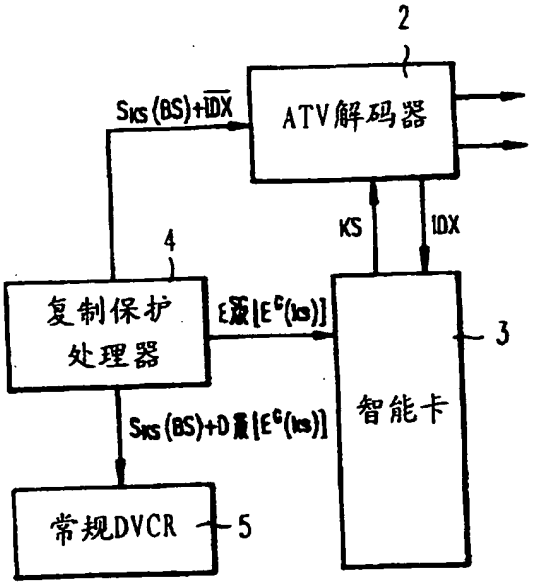

2
ATV解码器
KS
IDX
4
复制保护
处理器
3
智能卡
常规DVCR
5

图 18 b

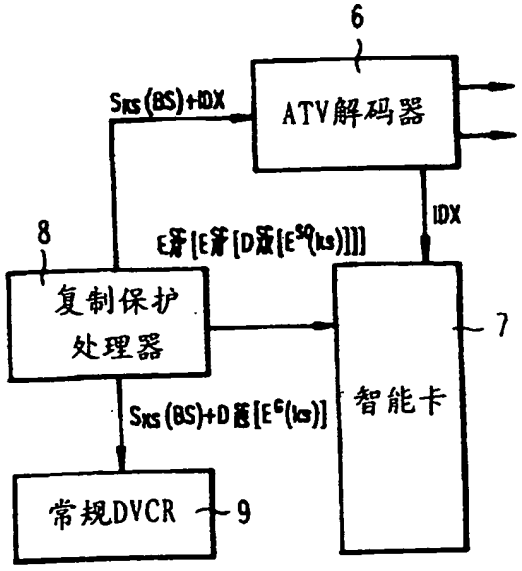

6
ATV解码器
IDX
8
复制保护
处理器
7
智能卡
常规DVCR
9

图 19 a

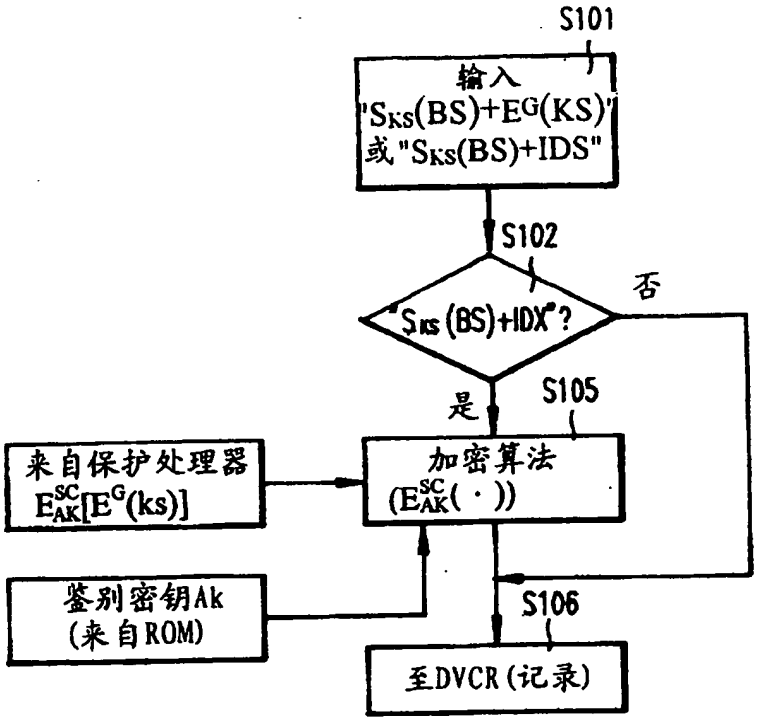
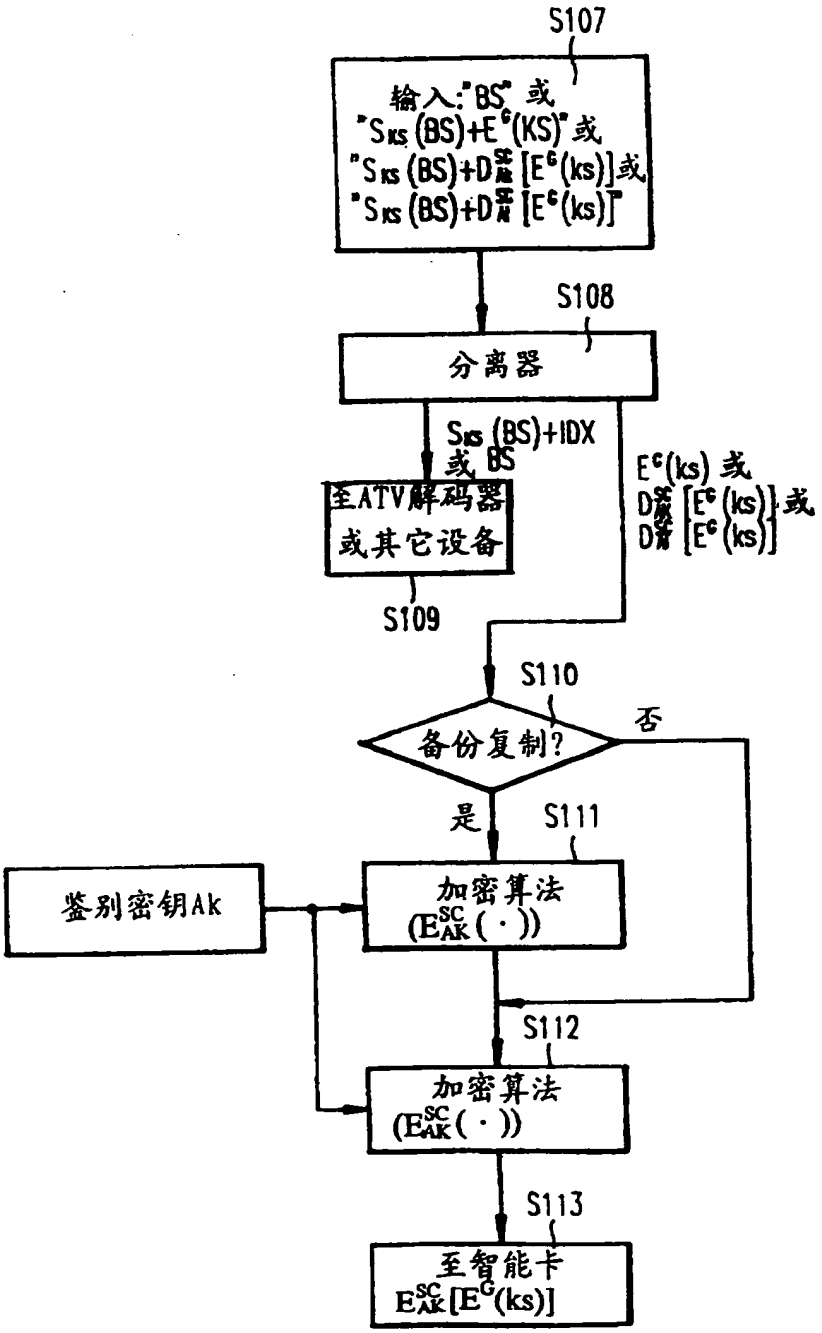

S101
输入
"SKS(BS)+EG(KS)"
或"SKS(BS)+IDS"
S102
SKS(BS)+IDX"?
否
是
S105
来自保护处理器
ESCAK[EG(ks)]
加密算法
(ESCAK(·))
鉴别密钥Ak
(来自ROM)
S106
至DVCR(记录)

图 19 b


S107
输入:"BS"或
"SKS(BS)+EG(KS)"或
"SKS(BS)+DSC鉴[EG(ks)]或
"SKS(BS)+DSC备[EG(ks)]"
S108
分离器
SKS(BS)+IDX
或BS
至ATV解码器
或其它设备
S109
EG(ks)或
DSC鉴[EG(ks)]或
DSC备[EG(ks)]
S110
备份复制?
否
是
S111
鉴别密钥Ak
加密算法
(ESCAK(·))
S112
加密算法
(ESCAK(·))
S113
至智能卡
ESCAK[EG(ks)]

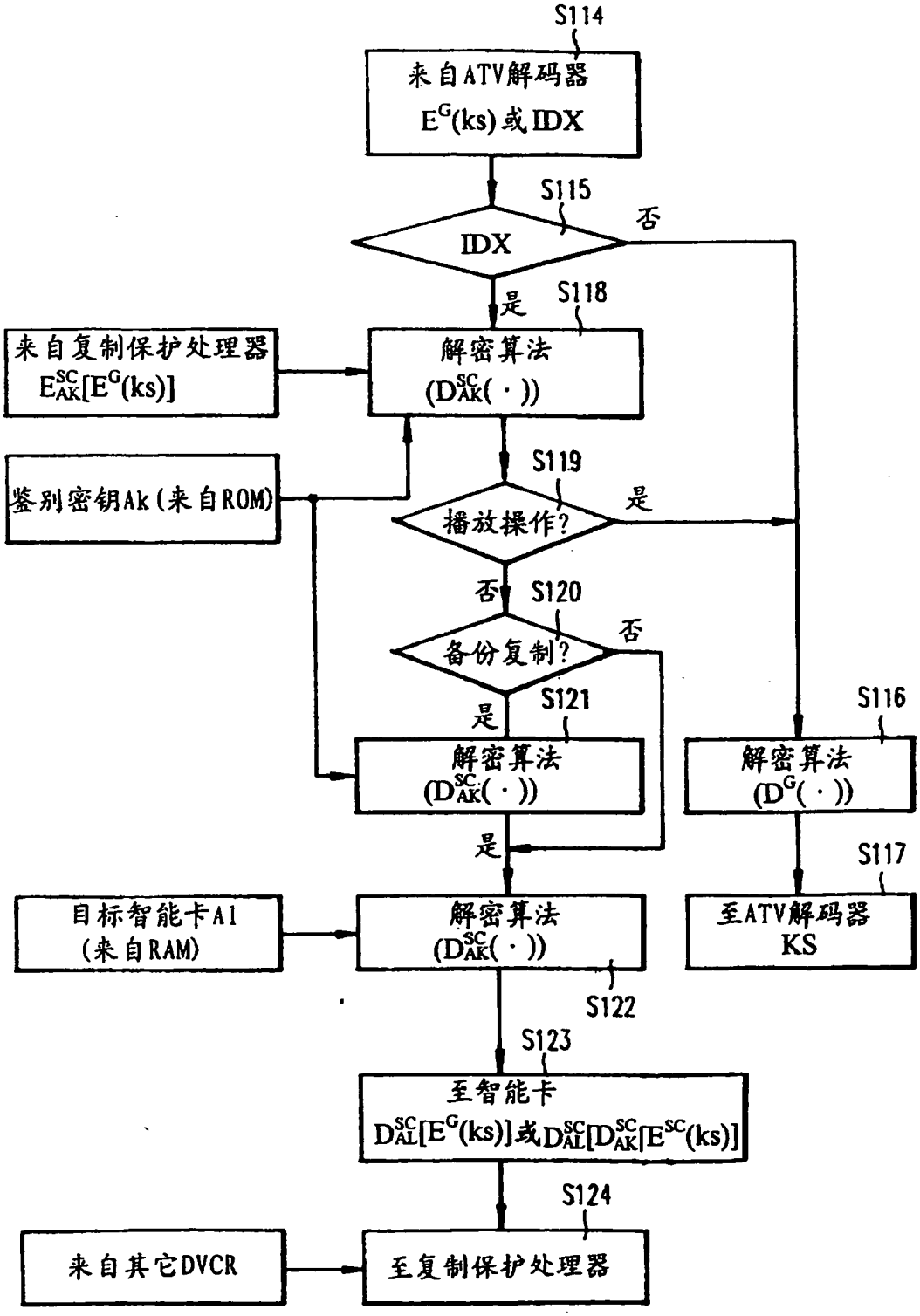
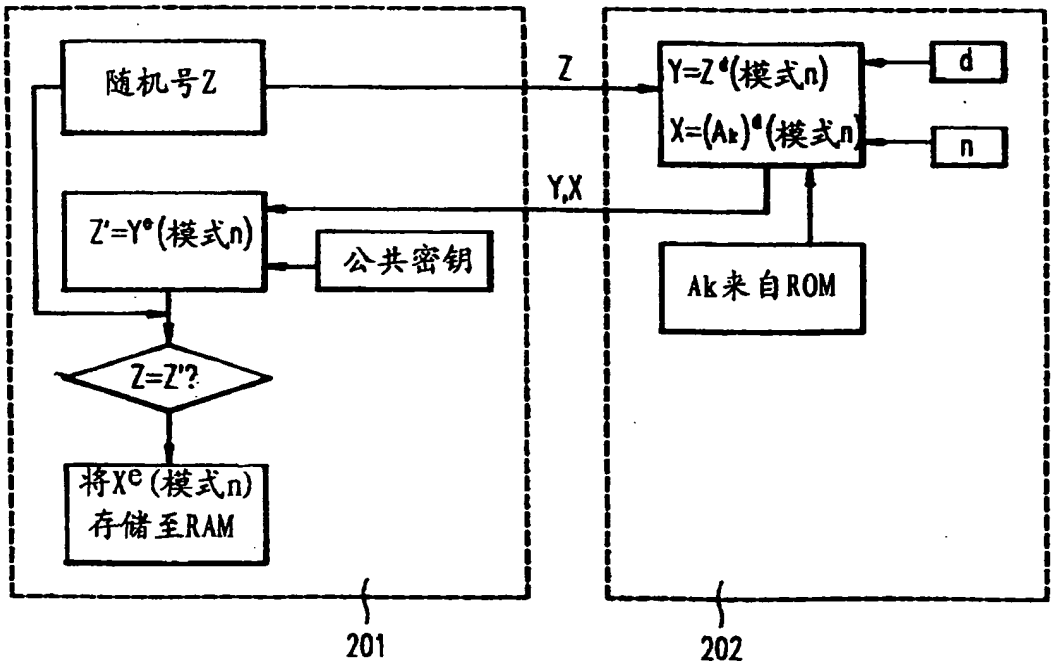

S114
来自ATV解码器
$E^G(ks)$或IDX
S115
IDX
否
是
S118
来自复制保护处理器
$E^{SC}_{AK}[E^G(ks)]$
解密算法
$(D^{SC}_{AK}(\cdot))$
鉴别密钥Ak(来自ROM)
S119
播放操作?
是
否
S120
备份复制?
否
是
S121
解密算法
$(D^{SC}_{AK}(\cdot))$
S116
解密算法
$(D^G(\cdot))$
是
S117
目标智能卡A1
(来自RAM)
解密算法
$(D^{SC}_{AK}(\cdot))$
至ATV解码器
KS
S122
S123
至智能卡
$D^{SC}_{AL}[E^G(ks)]$或$D^{SC}_{AL}[D^{SC}_{AK}[E^{SC}(ks)]]$
S124
来自其它DVCR
至复制保护处理器

图 20

图 21


随机号Z
Z
Y=Z^e(模式n)
X=(Ak)^e(模式n)
d
n
Y,X
Z'=Y^e(模式n)
公共密钥
Ak来自ROM
Z=Z'?
将X^e(模式n)
存储至RAM
201
202